IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON GREEN INTERNET OF THINGS

Received August 15, 2019, accepted August 29, 2019, date of publication September 6, 2019, date of current version September 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2939883

Building Reliable Routing Infrastructure for Green IoT Network

RAKESH KUMAR LENKA[1], AMIYA KUMAR RATH[2,3], AND SURAJ SHARMA[1]

[1]Department of Computer Science and Engineering, International Institute of Information Technology (IIIT) Bhubaneswar, Bhubaneswar 751003, India
[2]Department of Computer Science and Engineering, Veer Surendra Sai University of Technology (VSSUT), Burla 768018, India
[3]National Assessment and Accreditation Council (NAAC), Bengaluru 560072, India

Corresponding author: Rakesh Kumar Lenka (rakeshkumar@iiit-bh.ac.in)

This work was supported by the IoT and Cloud Computing Lab, IIIT Bhubaneswar.

ABSTRACT Present research work on the Internet of Things and Fog computing has taken hype due to the low cost of building them by optimized sensors. Wireless sensor devices play a vital role in developing IoT sensing infrastructure. These devices are connected to form a network known as the WSN assisted IoT network. The number of things is verdant in IoT creates an immense energy need. So, efficient energy utilization is required to alter the green IoT environment. These sensor devices are having limited power and computational capabilities. We can use energy-efficient data routing protocols as data transferring with these low powered sensors is very challenging. One may use the sensors for more time in sensing the environment and sending the information. This proposed protocol deals with a reliable routing protocol for IoT sensing Infrastructure. Initially, a rendezvous region was created in the middle of the network area. Clustering and multipath technique are used because it reduces energy consumption and increases reliability. The proposed protocol is simulated within Castalia simulator for attaining the performance beneath different characteristics like packet delivery ratio, the average energy consumption, end to end delay, and network lifetime. It is observed that the suggested technique is useful in energy consumption and helps in boosting the IoT infrastructure network lifetime.

INDEX TERMS Internet of Things, hot spot problem, WSN-assisted IoT, routing protocol, green IoT.

I. INTRODUCTION

I oT is a universal networking setup with unique configuration abilities as per regular communication practices. It utilizes an intellectual platform which impeccably unified in the network. It is one of the growing fields where trillions of devices get connected through the internet for the exchange of information. These devices intelligently sense the environment, automatically collect the data, and deliver the information to paired devices. Currently, we have realized a broad acceptance and deployment of IoT infrastructures and systems in several applications. It includes smart cities, logistics, and health care; which has higher demands for services in cloud data centers. It creates robust combination requirements between IoT and cloud services with data storage, processing, and management. Cloud services are advanced, which deliver flexible data computation and management for IoT capabilities. IoT has a capable prospect to form popular industrial applications and systems by influencing the emergent permeating of wireless sensor devices [1].

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

Common physical objects with benefits of sensor network and RFID are linked, monitored, and coped with the distinct system. Let us take an example of a smart phone; it has a huge number of sensors because it knows if you are moving, how you are holding it, it knows for how much distance from your face it is, it has even an eye to see the surrounding and to communicate in WSN. Nowadays thing starting from the household to transportation, health care to farming everything becoming smarter by making it an IoT product.

In today's scenario, there are several things on the web than folks. Currently, we have ten billion devices and expected to fifty billion devices by 2020. The technology that inherits in IoT can sense, communicate, acquire data to build a system that delivers better health care, safety, comfort, convenience, and wisdom. Hence, to fulfill the requisite demands, the IoT devices need to communicate with WSN [2], [3]. Acronym and definitions are provided in the Table. 1. List of Notations and definitions are provided in Table. 2.

The four Layers of WSN assisted IoT infrastructures was shown in the Figure 1. These layers are listed below:

1) Sensor Connectivity and Network Layer
2) IoT hub (Gateway) Layer

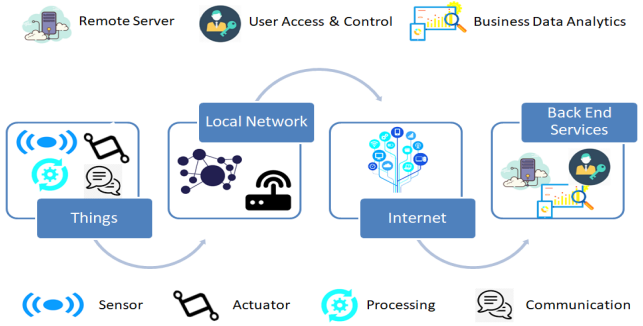

FIGURE 1. IoT Architecture.

TABLE 1. List of Acronyms and Corresponding Definition.

Acronym	Definition
IoT	Internet of Things
WSN	Wireless Sensor Network
RFID	Radio Frequency Identification
LBDD	Line Based Data Dissemination
RRP1	Ring Routing Protocol
RRP2	Railroad Routing Protocol
QDD	Quad Tree Based Protocol
CBRP	Centroid Based Routing Protocol
CH	Cluster Head
SCBC	Sector Chain Based Clustering Routing Protocol
BS	Base Station
LEACH	Low Energy Adaptive Clustering Hierarchy

3) Internet and Management Services Layer
4) Application (Back End Services) Layer

The Sensor Connectivity and Network Layer consist of the sensor network, sensors, actuators, tags (RFID, Barcode). The IoT hub (Gateway) layer deals with connecting the sensor devices to IoT hub and the gateway control. It includes technology such as Wi-Fi, WAN (GSM, UMTS, LTE, LTE-A). The internet and management service layer includes device modeling, configuration management, data flow management, and security control. The application layer includes various applications that can be built around the WSN assisted IoT networks such as environmental monitoring, object tracking, health monitoring, transportation, retail supply chain, etc.

The autonomous sensor-equipped device is the major component of WSN assisted IoT infrastructure. The data captured by the device are sent to the external system, which acts as data storage and manages the center. So the IoT devices can be deployed in a WSN infrastructure to communicate between themselves, and it is called WSN assisted IoT infrastructure. The number of things is increasing in IoT, which creates a massive energy need [4], [5]. So efficient utilization of energy is required to alter the green IoT environment [6]–[8]. It is important to extract the data which is required for the user and make it available [9], [10].

The IoT hub is responsible for connecting and monitoring the different type of IoT devices. It establishes the connection with the devices, collects all the real-time information and stores properly. The IoT devices required to find an optimal path to connect with the IoT hub, it may be directly or through the intermediate devices. It becomes easier due to the advancement of IoT hardware capabilities, but the constraint is the battery capacity of the devices. The IoT devices are used in certain applications where the device is deployed in a difficult geographical location. The battery cannot be replaced easily and immediately.

Due to the constraints like limited energy, limited memory, and computation power; the adaptation of IoT technology becomes difficult. Provision of global IDs for IoT device

TABLE 2. List of Notations and Corresponding Definition.

Notations	Definition
n	Number of IoT devices in the network area
(a_i,b_i)	Location information of IoT device i
d	Distance in meter
d_0	Threshold distance
t	Pause time of the mobile IoT hub
w_d	Width of the vertical and horizontal strip
(P_{max},Q_{max})	Maximum range of the network plane
$DNBR\_CTRL$	Peer discovery broadcast control packet
$DNBR(a)$	Group of IoT device which are peer of device a
$DNBR_{TABLE}(a)$	Peer table of IoT device a
RE_a	Residual energy of any device a
$DCTRL\_Sent_a$	control packet
w_{hor}	Horizontal range of the rendezvous area
w_{ver}	Vertical range of the rendezvous area
DEV_Pri	Devices used in the primary path
DEV_Alt	Device used in an alternative path
(a_{ch},b_{ch})	Coordinate of CH
$E_{Trans}(n,d)$	Energy cost to transmit n bits of data over the distance of d meters
$E_{Recv}(n)$	Energy cost to receive n bits of data over a distance of d meters
E_{Embb}	Energy cost for embedded circuit to receive or transmit a signal of one bit
E_{Amp}	Energy cost of the amplifier to preserve the radio reliable transmission
E_{fs}	Energy cost of the amplifier to transmit one bit at open space
α	Path loss exponent
E_{mp}	Energy cost of amplifier to transmit one bit at multi-hop model
E_{sleep}(t)	Energy spent by IoT device in sleep mode

is challenging. In recent years, many numbers of routing protocols have been proposed. These protocols are used for routing data from source to IoT hub to avoid constraint of energy inefficiency. The hotspot is another challenge that is, being present in the WSN assisted IoT network. In the WSN assisted IoT network, the devices that are present nearer to the IoT hub spent more energy compared to others because of the large computation [11], [12], [30]. To avoid such a condition, mobile IoT-hub is proposed. The IoT devices are used either for sending or transfer the data from one device to another, resulting in more energy consumption and increased network lifetime. So the routing protocols need to use an efficient routing technique to ensure that optimized energy is spent in sensing or transferring the data [14], [15], [16].

There are issues involved in the mobile IoT hub. The mobile IoT hub changes its position frequently, so it needs to inform all the devices in the network to establish a routing path. It leads to an increase in energy consumption overhead, which builds the network very dynamic [17], [18], [19]. Therefore, a routing path search before the requirement is an issue. The most recent data is more important in some event-based applications like fire detection, smoke detection, intruder detection system, security system, health tracking, target tracking. Hence, the end to end latency is required to be reduced for a better protocol.

It has been observed that the scalability is also an issue for the event-based applications. We can observe from many cases that a single bit of data loss can lead to a massive problem for the particular application. As these devices are deployed in steep terrain, there might be a possibility that any number of device dies at a specific time due to the particular natural incidence or any unexpected situations [20]–[23]. Even if a single device dies, that will bring a huge loss for the system. For that reason, it is necessary to create a dynamic route from the source to the IoT hub [24]–[27]. Afterward, if any device dies within the previous route, an alternate routing path will be available instantly. Also, it mustn't spend additional energy for this process resulting in reduced network life [28], [29].

The Figure 2 shows the applications of IoT from different domains that suit WSN assisted IoT architecture. Some of the key applications are listed below:

A. SMART WATER MONITORING

IoT helps to monitor water management with the aid of WSN. Water quality parameters like pH, Turbidity, temperature, conductivity, dissolved oxygen, and free residual chlorine are monitored; further informed the authority and consumers. The sensor data at the water network are wirelessly communicated to the central server. It helps to manage to prevent water leakages and the Flood.

B. SMART AGRICULTURE

The sensors (light, humidity, temperature, soil moisture, etc.) are established in the farming area for monitoring of the crop field. It automates the irrigation system, which helps the farmer to monitor the field condition anywhere. It mitigates the challenges arising from situations based on climate change and extreme weather conditions.

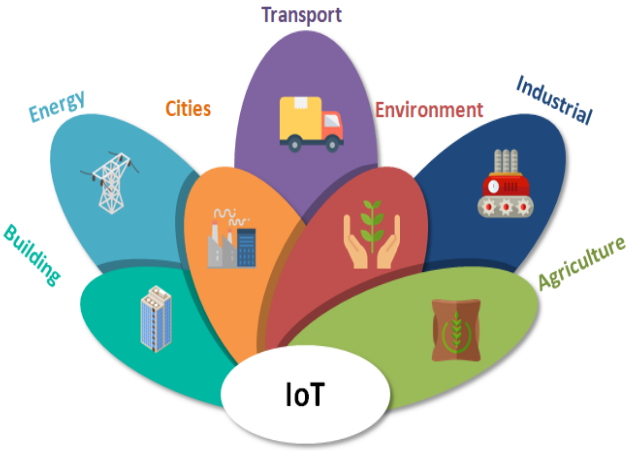

FIGURE 2. Applications of IoT.

C. SMART LIVING

Smart Home helps in monitoring the household assets wirelessly. It has the provision for auto-switching (on/off) of the available appliances (TV/Refrigerator/Air-conditioner, etc.) in the home to prevent wastage of electricity. It provides real-time information on the usage of gas lines by connecting residential gas meters to an Internet protocol (IP) network lead to a reduction in labor and maintenance cost.

D. SMART ENVIRONMENT MONITORING

The Drone-based sensors can capture air pollutant emission and measure the requisite components to facilitate the user regarding air pollution. It prevents substantial contamination and related disasters. The user can also obtain local data for production monitoring, problem detection, and local climate control. It helps to detect forest fire, prevent landslide, earthquake, etc. and protecting wildlife. It also helps to reserve the arts and monuments in museums.

The key contributions of this paper can be summarized as follows:

1) We have investigated the important facets of IoT, where efficient utilization of energy is needed to enable a Green IoT environment. We have done a survey on recent advances in various sensing schemes in WSN assisted IoT networks.
2) The state-of-the-art routing schemes, such as schemes like LBDD [30], Rendezvous-based routing [31], RRP1 [33], RRP2 [34], QDD [35], CBRP [36] and SCBC [37] has been explored to identify their limits and challenges to provide a new research avenue.
3) We have developed a novel routing scheme for the WSN assisted IoT infrastructures. We have created a rendezvous area within the network. We have applied the clustering technique in the rendezvous area as it is

an important method for prolonging the network lifetime. Further, a treelike structure within the rendezvous region to provide reliable communication.

4) Two modes of data transmission have been used to show the protocol performance in various scenarios. In the first approach, the data transmission takes place from the source to the hub via the coordinating devices, whereas the second approach involves the direct information transmission from source to the hub through the intermediate devices by using location recovery technique.
5) The proposed protocol is tested on both real and synthetic data of a WSN. The protocol efficiency can be accessed by comparing the protocol performance on the characteristics such as the network lifetime, average energy consumption, end to end delay, and packet delivery ratio.
6) Simulation results clearly illustrate that the first routing framework beats the current protocols in parameters like end-to-end latency and delivery ratio. The second proposed routing framework provides significant gain in energy saving. Thus, it can serve as a benchmark for the realization of routing operations of WSN assisted IoT applications. Further, the treelike structure within the rendezvous region insights on the impact of the proposed routing framework on reliable communication, which has been missing in the previous schemes. Superior energy-saving and reliable communication guarantees of the proposed scheme over the widely used routing schemes.

II. RELATED WORK

In latest years, various routing protocols have been proposed for WSN assisted IoT Networks [32]. Out of these varieties of the new protocols, some are discussed in the next section.

Generally, in most of the WSN assisted IoT network, the transfer of information takes place from the IoT devices (sensors) towards an immobile IoT hub (base station). In LBDD routing protocol [30] the IoT Hub is mobile. At first, the network area is split into two equivalent fragments. The network area is further divided into clusters, with every cluster having size g. The IoT devices that fall inside this virtual line is named as the inline devices. Every device realizes its geographical area just as the system geographical limits. It is assumed that we have multiple mobile sinks moving haphazardly within the network area.

The LBDD involves two steps: data dissemination and data collection. In the first step, the ordinary devices are used for sensing data and sending to the closest inline device. In the second step, the IoT hub wants information; it sends a request to inline devices. The first inline device which gets this inquiry passes it in two directions along the virtual line until it approaches the inline device, which contains data. Once getting the query, the inline device transfers the data to the IoT hub. It accepts the data only if data are non redundant.

Two techniques can be used to facilitate the information query process. The first methodology needs a calibrating of w and g to keep the system under control during high traffic load. The second method needs time to time election of the group head.

When the amount of queries is more than the data, the duplication of data in the vertical virtual line helps in reducing the overall energy consumption and system overhead. It is possible that at times, the queries outnumbers the data packets. LBDD queries are propagated along the line. The overhead for establishing the line structure is low. The width of the line should be enough to diminish hotspots problems. Due to this energy consumption is reduced.

In most of the WSN assisted IoT network the energy of the devices which are closer to the IoT hub depletes quickly as compared to other devices. This happens because the more amount of data is concentrated around the IoT hub which in turn interrupts the communication between the device and IoT hub. To reduce this problem, the concept of mobile IoT hub was introduced. This helps in reducing energy consumption and balanced data transmission.

Ring Routing [33] protocol (RRP1) comes under the area based routing protocol. The IoT devices in the entire network region are grouped into three categories. The devices which come under the virtual ring structure are known as the ring device. The ring device stores the position of the Anchor devices. Anchor devices store the location information of IoT hub. The regular devices want to send the data to the IoT hub. The ring radius to be constructed is defined initially, and the IoT devices at this radius are called ring IoT devices. Any IoT device at this distance uses the concept of geographic forwarding in any direction following a greedy approach for the selection of ring IoT devices until a closed loop is formed leads to the ring construction. The portable hub chooses another device as an anchor device whose primary responsibility is to receive and pass on the device information to the hub. When the hub's location information becomes outdated, the sensor device data are passed on to the new anchor device through the old anchor device. The new anchor device pass on the device data to the hub. It forms a structure almost like the shape of a ring or closed loop. After the network organization, an underlying radius is decided. Devices of IoT falling within this radius are called as ring devices. Ring devices help ordinary devices for obtaining data concerning the hub's new position. At first, the devices nearest to the hub is picked as an anchor device. The hub broadcasts an anchor device selection packet following the selection of anchor device. Using anchor device position information packet, the hub alerts the ring devices regarding the anchor device. The hub within the ring share data with neighbors after accepting the ANPI packet.

The source device requests the position of the anchor device. The ring devices respond to it by sending the anchor device position information packet. After getting the location information of the anchor device, the source device transmits the data to the anchor device. The effects of control packets are reduced by consolidating the minimal number of sensor

devices inside the closed-loop. The RRP1 protocol works with insignificant wasteful broadcasts.

Ring Routing doesn't rely heavily on broadcasting; hence, it's appropriate to be used for sensor devices using offbeat MAC protocols supposed for WSN assisted IoT networks. The RRP1 protocol gives fast information conveyance owing to the speedy openness of the proposed ring structure that enables the protocol to utilize for time-delicate applications. It doesn't need data regarding the movement of the hub for RRP1 to work. It doesn't rely upon foreseeing the hub's direction and reasonable for the irregular hub portability situations. The RRP1 protocol is fair for both event-driven and occasional information revealing applications. Since RRP1 protocol isn't a query-based protocol, information can be transmitted as soon as they are produced. The number of routing packets is reduced in the RRP1 protocol by maintaining a minimum number of devices in the ring. The minimal inefficient broadcast is employed in ring routing.

The basic idea behind Railroad Routing [34] protocol is that the likelihood of occurrence of event generation in the network is uniform. Rail infrastructure is exploited by Railroad protocol, which stores all the information of event data. The devices within the rail are known as rail devices. The ordinary devices sense data and the corresponding metadata are forwarded to the closest station that should be a rail device; the platform devices are the ones which are part of the station. The construction of the rail occurs during the network setup.

For a device to know if it is part of the rail, it should have known about its distance from the network center and the closest boundary device. The rail is alert about event summary using the event notification message. The rail device receives the message, and it is forwarded to platform devices on the new station. In this protocol, a virtual framework called Rail is set up which contains the meta data of all the events occurring in the system. The Rail is located at the center of the network so that all devices can have equal access to it. The sensor devices which are present inside the Rail are called as Rail devices. A group of Rail devices together forms a station. Every station consists of many devices, and these devices are called platform devices. Every device within the network has information about its geographic location.

There are four basic operations performed in Railroad routing: Rail construction, notification of events, query request and delivery of data. There are three structure parameters to develop Rail to accomplish the objective; the depth of Rail, the width of Rail, and the stations. The construction of Rail takes place during the network setup phase. When an event is detected, the device stores the data and passes it onto the nearest rail device. The hub gets information by sending a query. It is sent to source in three stages: Query advertising on the rail, circulation of query through the rail, inquiry notice to sender device. IoT hub sends an inquiry to its neighbor devices and later on intermediate devices forward it to the rail. When the query reaches the rail, it flows around the rail with the assistance of directional data. It likewise analyzes all the stations in the middle of its track. On the off chance that any station has essential information that hub needs, then the platform device sends an inquiry warning message to the initiating device. In the wake of getting the query notification message, the source device sends the information to the hub.

Upon receiving the query alert message, the message is directly sent to the hub from the source. A hub can discover every bit of information with an intermediate of Rail without stretch. It is pointless to broadcast a query or make a muddled structure to discover information of interest. Railroad expends substantially less energy and in this way expands the system's lifetime. Railroad differs from LBDD by using unicast while sending the query of the hub, unlike the LBDD which broadcast the packets. The station should cover the whole dimension of the rail to ensure that a device with metadata from the query isn't missed. Delay in the transmission of data is comparatively more than LBDD as the query has to cover a longer distance.

In Rendezvous-based routing [31], a rendezvous zone is constructed at the center of the network area, and a tree is built inside that network area. In this routing protocol, it is assumed that the sensor devices are immobile after installation. The hub is mobile within the boundary of the network. The hub has infinite battery power and computational capability; each device has its unique identification number and information regarding their remaining battery life. The sensor device is randomly and uniformly deployed within the network area, the sensor devices have a limited lifetime, and the data transfer rate is uniform across the network. A virtual, hybrid region area of width w, comprising of horizontal and vertical zones is built in the middle of the network area. The whole network area is divided into four sections: horizontal left, vertical up, horizontal right, vertically down, and the intersection of this section acts as the rendezvous zone. The sensor devices present in the rendezvous zone are classified as the backbone devices. The tree which is built inside the rendezvous zone helps in transmitting the information from the source to the hub and contrariwise. All the devices which are responsible for the construction of the tree know the exact location of the hub. The devices inside the rendezvous zone have no prior information of the hub's location.

In the system, we have one hub and n number of devices. In the network, the sensor devices are immobile, and the hub moves at a speed of 5 m/s to 30 m/s. A delay time δ for the hub is taken into account to gather the information. The vertical zone of width w is located in the middle of the network space. When an IoT device senses any information, it directly reports it to the hub. The Random Way-point model takes into account for the hub's mobility. The devices can discover their geographic location at any time, and also the device can differ its transmission run-up to the foremost extreme range R. The minimum residual energy of a sensing device is termed its threshold energy. Beyond its threshold energy, a device can't perform any other task other than sensing and transmitting the data.

A WSN assisted IoT network consists of various sensor devices that are deployed to observe and communicate with the real world. Since every sensor device can partially perceive the expansive landscape, so they should work together for the productive and dependable conveyance of factual information to the IoT hub. The basic idea behind the quadtree-based routing protocol is to take advantage of the quadtree-based network area partitions. The quadtree-based routing protocol (QDD) [35] is an efficient protocol that underpins stimulus as well as hub mobility. This protocol is designed for sensor devices having a fixed geographic location, but in a few cases, the stimuli and the hub could also be mobile. Every IoT hub realizes the entire sensor field space zone N where N is defined as $2^m \times 2^m$; where $m = \log_2 N$. This protocol uses a greedy geographical forwarding technique for data and query transmission. A sensor device is chosen as the root of the WSN assisted IoT network. The sensor field space N is divided into four quadrants. All four quadrants are considered as the child of N. Each quadrant is further divided into four sub-quadrants, and each sub-quadrant have their root device. After identifying a stimulus, source device S plays out a legitimate apportioning of network area as mentioned.

While sending data packets, each device keeps up a routing table. The table entries include the location and identity of the source device, message, previous device info, packet type, sequence number so that duplicated listings can be identified and dropped eventually. Each table section incorporates a lapse field that decides to what extent that packet would stay legitimate before it is disposed from the table. This protocol has lower average energy consumption and better packet delivery ratio as compared with the existing alternative hierarchy based routing protocols. This protocol gives a productive answer to the portable stimulus sink problem by making the information transmission process autonomous. QDD doesn't address the hotspot problem in case of loop falls.

In Centroid-Based Routing Protocol (CBRP) [36] energy efficiency was proposed to be increased in the data routing protocol, which employed a sensor device to enhance the network performance. The clustering is completed based on the distance from the Base Station (BS). The energy is uniformly distributed through the network by choosing a device as Candidate Cluster Head (CH) device. Clustering overhead is reduced as the BS is made responsible for its formation. BS sets a threshold distance limit beyond which the packets cannot be transmitted. In the latter case, there is a loss of data. There was no defined procedure for the reelection of a cluster head in this protocol. This protocol uses energy efficiently for data routing to enhance the performance of the whole network. The devices don't change their position after the setup phase. The devices have complete information regarding their location. At any instant of time, any device has location information and the energy level of the hub. The cluster head has direct communication with the hub. The hub is responsible for dividing the sensor field into clusters. The energy is distributed uniformly across the network. There are three necessary steps involved in centroid based routing: setting up phase, selection of cluster head, and rotation phase. During the setup phase, every device sends its location information to the hub. After getting the device's location, the BS selects the CH based upon their energy state and also the distance from the BS. It reduces the overhead of cluster formation.

The CH broadcast their identity and location information to all their neighboring devices after the selection phase. The CH calculates the location of the energy centroid of the cluster. The device closest to the energy centroid is elected as the candidate CH. The network coverage increases significantly as the candidate CH is close to the energy centroid. The candidate CH is chosen during the rotation phase. For transmission of data packets, this protocol uses a threshold distance. The data packets get lost if the distance becomes more than the threshold distance. The procedure of re-appointment of cluster head has not been characterized. As far as scalability, overhead, life cycle, computations, mobility is concerned, this protocol performs better than LEACH protocol. This protocol solely works when sensing devices are immobile.

In Sector Chain Based Clustering Routing Protocol (SCBC) [37], the network space is divided into sectors. The number of sensing devices in each sector is uniformly distributed. Each sector has one cluster head (CH). It is assumed that the network contains ordinary devices, advanced devices, and super devices with different energy levels. All the sensing devices and the hub are immobile. All the communication links have bidirectional nature. The basic operations performed in this protocol are: setting up the network and transmission of data. During the setup phase, the hub collects the information such as geographical location and remaining energy level of each device. The CH is chosen with the idea of the residual energy state of the device. Secondary CHs are selected to transmit packets to the hub so that the energy of CH can be saved. The distance between the hub and the secondary CH is minimal. It develops a chain for every sector with the CH as the chain head and secondary CH that has high leftover energy. It uses time division multiple access techniques for the transmission of data packets. Each sensor device forwards it's sensed data to the next device within the given time slot. Initially, the most remote device in the chain will begin transmitting sensed data to its neighbor device. The devices present in the center of the chain get packets, combine one or more data packets with its very own into a single parcel and send it to the subsequent device or CH or secondary CH along the chain. After receiving all the data packets, the secondary CH aggregates the data packets and forwards it to the BS.

This protocol makes efficient use of energy. The total network energy dissipated significantly reduces because it uses chains for data transmission. Since the network space is split into sectors, the lifetime of the network can be increased by proper balancing of devices within the network. The packet delivery ratio, throughput, end-to-end delay of the network

is better in compared with protocols that using sector (chain) based architecture.

III. PROPOSED WORK

The routing in WSN assisted IoT networks has become a crucial issue in these days. The IoT devices monitor the data from the environment and transmit it to the IoT hub. It includes several intermediate IoT devices to forward the data. In contemporary application, the IoT hub needs to be more mobile instead of static. In specific applications, the regular supply of energy to the IoT device isn't attainable. So energy, efficiency, and reliableness became a pressing concern to develop an efficient routing technique that prolongs the network lifetime and increase the reliability. This paper projected a reliable rendezvous routing protocol for IoT sensing infrastructure. We have created a rendezvous area within the center of each horizontal and vertical directions. We have created a cluster within the rendezvous area and additionally created a treelike structure within the rendezvous region. Here we have projected two ways of information transmission between the source and the IoT hub. One path is through the rendezvous region tree devices, and in another technique, IoT hub updates its location information to tree device. The source device gets location information of hub from the closest tree device and sends the information on to the hub through the intermediate devices.

A. ASSUMPTIONS

1) The IoT devices are stationary in the network plane.
2) The IoT hub is mobile.
3) The IoT devices are randomly deployed in the network but follows a uniform distribution.
4) The IoT hub has an unlimited supply of energy, computation, and storage.
5) Each IoT device contains its ID and can calculate its residual energy.
6) IoT devices are identical, i.e., same computational capabilities.
7) IoT devices have a certain amount of energy.
8) The speed of data transfer is the same in both directions over the average time through the link.

B. PEER DISCOVERY

In this section, each IoT device discovers its peer device. The device that starts the process of peer discovery broadcast a control packet (*DNBR_CTRL*). This packet has the device *ID*, residual energy status, and coordinates of the device. The devices which receive this (*DNBR_CTRL*) control packet maintains a peer information table which contains the device *ID* of the sender, its residual energy state and coordinate. If the receiver already has the device *ID* inside its peer information table, then it will drop that packet. The recipient device which receives the (*DNBR_CTRL*) packet also broadcast the (*DNBR_CTRL*) packet if it has not broadcast previously. Subsequently, this process continues until every device has its one-hop peer information.

Algorithm 1: Peer Discovery

1 $DNBR(a)$: Group of IoT device which are peer of a initialized to ϕ.
2 $DNBR_{TABLE}(a)$: Peer table of IoT device a initialized to ϕ.
3 RE_a: Residual energy of any device a.
4 $DCTRL\_Sent_a$: Set to true when the IoT device a sends *SNBR_CTRL* packet. Initialized to false.
5 POS_a: Position of device a.
6 IoT device a receives packets from IoT device b.
7 $DCTRL$: <DCTRL, id_b, RE_b, POS_b>
8 **if** $b \notin DNBR_{TABLE}(a)$ **then**
9 $\quad DNBR(a) = DNBR(a) \bigcup$ b ;
10 $\quad$ Update $DNBR_{TABLE}(a)$ with <id_b,RE_b, POS_b>;
11 $\quad$ **if** $DCTRL\_sent_a == false$ **then**
12 $\quad\quad DCTRL\_sent_a \leftarrow$ true ;
13 $\quad\quad DCTRL$: <DCTRL, id_a, RE_a, POS_a> ; // ▷ Broadcast *DCTRL* packet
14 $\quad$ **else**
15 $\quad\quad$ Drop the packet;
16 $\quad$ **end**
17 $\quad$ Drop the packet;
18 **end**

C. RENDEZVOUS REGION FORMATION

The initial view of the network area is shown in Figure 3. In this proposed work, we partitioned the whole network space into four equal planes by one horizontal and one vertical strip. This horizontal and vertical strip is termed as rendezvous region.

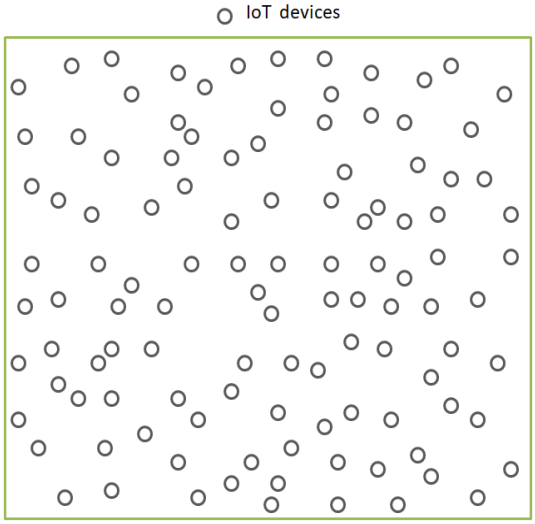

FIGURE 3. Initial view of sensor area.

Let w_d is the width of the vertical and horizontal strip,(P_{max},Q_{max}) is the maximum range of the network plane. The four coordinates of the network plane are shown

in Figure 4. The vertical and horizontal range of the strips w_{hor} and w_{ver} are defined as in the equation below

$$w_{hor} = (P_{max} - w_d)/2 \; to \; (P_{max} + w_d)/2 \quad (1)$$

$$w_{ver} = (Q_{max} - w_d)/2 \; to \; (Q_{max} + w_d)/2 \quad (2)$$

The IoT devices present in that area are called backbone devices.

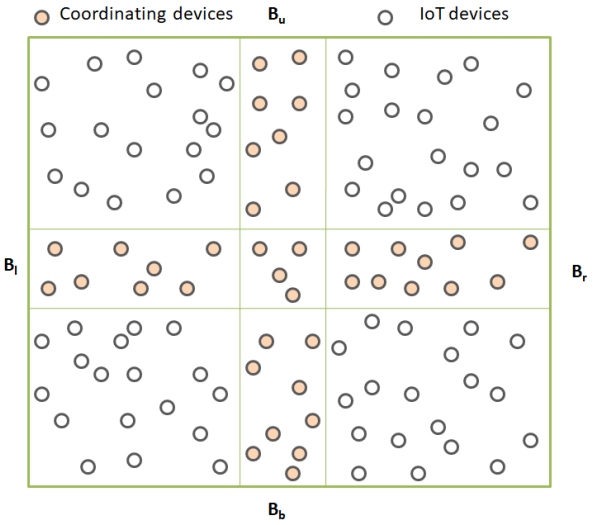

FIGURE 4. Rendezvous area with backbone devices.

D. GROUPING OF FRIENDS INTO CLUSTERS

The formation of cluster occurs inside the intersection region of both horizontal and vertical stripe:

1) The process of cluster formation is started by device m, which is having a high node degree which is connected to more number of peer devices and also having residual energy level more than threshold values. If a device having high node degree and residual energy less than the threshold value, go to step 4.
2) Find the device z which has the highest maximum common adjacency among the friends of start-up device. The device with the lowest *ID* is taken into consideration if several devices are present.
3) The common one-hop peers of both m and z come under one cluster with devices m,z included and device m will be considered as the new cluster head (CH).
4) Same method of cluster formation is followed by the leftover one hop peers of start-up device m having a maximum node degree and announce itself as CH.

The complete process of cluster formation is illustrated in the Algorithm 2 given below:

Figure 5 shows the clustering process among the coordinating devices. As per Algorithm 2, the device A starts the cluster formation technique because it has the highest degree. The device D has the most common adjacency with the initiating device A. Hence, the devices (A, B, C, D and E) forms one cluster and the device A becomes the new CH,

Algorithm 2: Grouping of Peers Into Clusters

N: Total device count in the entire IoT frame infrastructure (V_m,E_m) : Connectivity matrix of device m. V_m comprises of the device m, and it's one-hop neighbors. E_m comprises the duplex edge between the device in V_m.
m: Start up device
$S(m)$: group of neighbors of device a
$X(m)$: $X(m)$ comprises of one hop neighbor devices of device m
$C(m)$: group of elements in cluster which is empty at first.
N_$C(m)$: group of devices which are absent in cluster.
m $= max_{arg_n}$ degree(N_n) ▷n is any arbitrary device
$S(m) =$ {n,(m,n)$\in E_m$}, $C_m =$ {m}
foreach *device m in the network* **do**
  if $Er_m >$ *threshold energy* **then**
    while $X(m) \neq \phi$ **do**
      Search z $\in X(m)$ where $|X(m) \bigcap X(z)|$ with maximum;
      $C(m) \leftarrow [C_m \bigcup \{z\} \bigcup \{n,\{n,z\} \in E_m]$;
      count($C(m)$);
      N_$C_m \leftarrow [V_m \notin C_m]$;
    end
  end
  m $= \max_{arg_m}$ degree(N_C_m);
  CH $\leftarrow$ m;
end

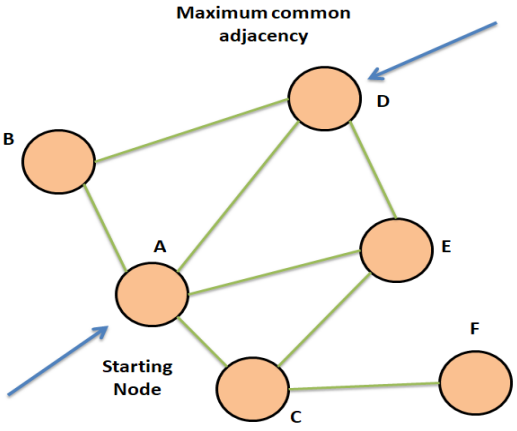

FIGURE 5. Clustering process.

whereas device D recaps the identical process to create cluster and become next CH. When any cluster head's energy falls below a threshold, a new device from that cluster can begin the cluster formation process if it's energy greater than the threshold level and it holds the maximum common adjacency.

E. TREE CONSTRUCTION

Tree formation is one of the important aspect of the proposed protocol. The multipath tree is formed inside the rendezvous

region by taking only backbone devices. To continue this process, we need to find out the four boundary devices. Initially we take four points in the IoT device boundary plane B_u, B_d, B_l, B_r. The coordinate of those points are (P_{max}/2,0), (P_{max}/2,0), (0,Q_{max}/2), (P_{max},Q_{max}/2) respectively. We initiate the process of finding four boundary devices from the boundary points by taking the IoT devices, which is in the smallest Euclidean distance from the boundary points.

Here B_u, B_d, B_l, B_r are four points in the boundary. We select four boundary devices BN_u, BN_d, BN_l, BN_r from these points. The process of tree construction initiates from these points. Every device of the network has data of its peer device that include device *ID*, residual energy, and coordinate in the plane. The boundary devices select the next device by taking the following conditions.

1) The device must be a coordinating device.
2) The residual energy level of the device must be greater than and equal to the threshold level.

The process of tree creation between the boundary devices and cluster head initiate as we get the boundary devices. Here we define two types of devices i.e., *DEV_Pri* and *DEV_Alt*. *DEV_Pri* are the devices used in the primary path, and *DEV_Alt* is the device used in an alternative path. In the case of choosing the primary path, the IoT device selects the next device, which has minimum DF and sufficient residual energy. In another case for choosing the alternate path, it selects the device with the next minimum DF and sufficient residual energy. The alternate device searches one device close to the cluster head.

The Process of device selection uses the following equations.

$$DF = \sqrt{(a_{ch} - a_i)^2 + (b_{ch} - b_i)^2} \tag{3}$$

$\forall a \in DNBR(j)$

where DF(j) is distance between the peer device (j) and the CH.

(a_{ch},b_{ch}) is the coordinate of CH.

(a_i,b_i) is the coordinate of any device *i*. *SNBR*(*j*) is the peer device of *j* whose residual energy is greater than equal to the threshold level.

Here, only the primary devices are active and rest are in sleep mode. So, the interference from other paths will absent. It will avoid collision and save energy. Once the primary path breaks, the proposed protocol will find an alternate path for communication. However, once all the paths break, it will start again from the process of peer selection. Figure 6 shows the tree construction in between the rendezvous region.

F. REGION DISCOVERY OF IoT DEVICES

The network plane is divided virtually into eight sectors, as shown in Figure 7. The sectors help the IoT devices to find their location in the network plane and their shortest route.

IV. ENERGY CONSUMPTION MODEL

To calculate the IoT device energy consumption, we should consider receiving and transmitting energy for IoT devices.

Algorithm 3: Tree Construction

DEV_Pri: It is used for the Primary device.
DEV_Alt: It is used for the Alternate device.
Pri_CTRL: It is the control packet broadcast by the primary device.
Alt_CTRL: It is the control packet broadcast by the alternate device.
DEV_BND: Set of backbone devices which are boundary devices.
Search_Pri_Path(): This function is used by both *DEV_Pri* and *DEV_Alt*.If the *DEV_Pri* uses it, It will broadcast its ID with *Pri_CTRL* packet for next primary device selection. If *DEV_Alt* uses it, it will broadcast its ID with *Alt_CTRL* packet for next alternate device selection. Here *DEV_Pri* construct the primary path and *DEV_Alt* construct the alternate path.
Search_Alt_Path(): This method is used by *DEV_pri*, to search an alternate path closer to the CH.
DEV_BND←*DEV_Pri*
repeat
  if *device*==*DEV_Pri* **then**
    Search_Pri_Path();
    Search_Alt_Path();
  else
    device==*DEV_Alt*;
    Search_Pri_Path();
  end
until *DEV_next*≠ *Cluster head*;
Function *Search_Pri_path* ( )
  if *device* == *DEV_Pri* **then**
    Broadcast *Pri_CTRL* Packet;
    Choose next device using equation and equation;
    DEV_next=*DEV_Pri*;
  end
  if *device* == *DEV_Alt* **then**
    Broadcast *Alt_CTRL* Packet;
    Choose next device using equation and equation;
    DEV_next=*DEV_Alt*;
  end
End Function
Function *Search_Alt_path* ( )
  if *device* == *DEV_Pri* **then**
    Choose *DEV_Next* accept it as Primary device using equation and equation;
    DEV_next=*DEV_Alt*;
  end
End Function

Let $E_{Trans}(n, d)$ is the energy cost to transmit *n* bits of data over the distance of d meters and $E_{Recv}(n)$ is the energy cost to receive n bits of data over a distance of d meters.

For transmitting *n* bits:

$$E_{Trans}(n, d) = E_{Embb} * n + E_{Amp} * n * d^{\alpha} \tag{4}$$

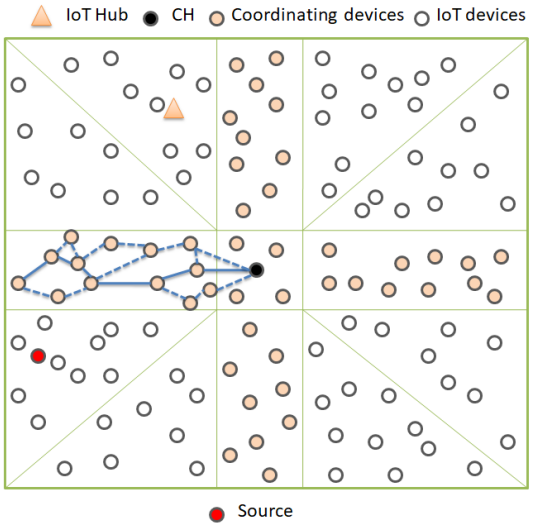

FIGURE 6. Tree construction in between the rendezvous region.

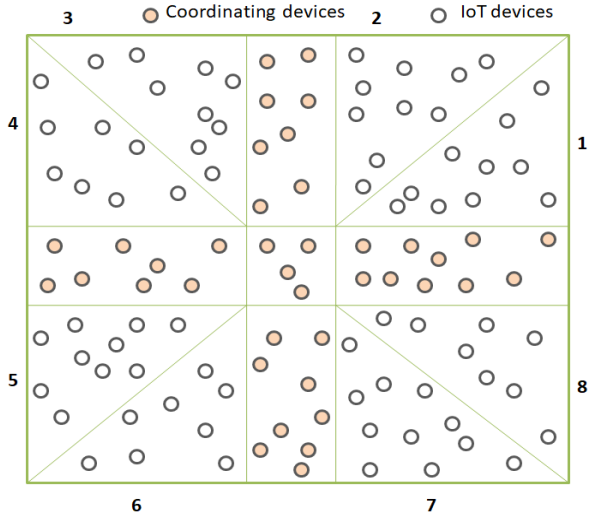

FIGURE 7. Region discovery for IoT devices.

Here E_{Trans} is the energy required for transmission, and d is the Euclidean distance between two devices.

For receiving n bits:

$$E_{Recv}(n) = E_{Embb} * d. \tag{5}$$

Here E_{Recv} is the receiving energy required. E_{Embb} is the cost of energy for embedded circuit to receive or transmit a signal of one bit. E_{Amp} is the amplifier energy consumption to preserve the radio reliable transmission.

Free space propagation model is used, the energy cost on amplifier E_{Amp} referred as:

$$E_{Amp} = E_{fs} \tag{6}$$

Here E_{fs} is amplifier energy cost to transmit one bit at open space.

Algorithm 4: Region Discovery for IoT devices

θ=0,β=0
(s,t): center of the network plane
(a,b): Any IoT device position in the network
Let $\pi = 180°$;
Center ← (s,t) ; // ▷*Center* is the middle point of the network area.
For any IoT device c in the network with position(a, b) let the new coordinate
(x,y) ←($a - s, b - t$) ; // ▷ Evaluate (X,Y) corresponding to the center.
$\theta = tan^{-1}|\frac{Y}{X}|$
if $X > 0$ && $Y > 0$ **then**
    $\beta \leftarrow \theta$;
    if $0 < \beta < \frac{\pi}{4}$ **then**
        device with position (a, b) is in the 1^{st} sector and the device can communicate from BN_r with destination point(a,t).;
    else
        if $\frac{\pi}{4} < \beta < \frac{\pi}{2}$ **then**
            device with position (a, b) is in the 2^{nd} sector and the device can communicate from BN_u with destination point(s,b).;
        end
    end
end
if $X < 0$ && $Y > 0$ **then**
    $\beta \leftarrow \pi$ - θ;
    if $\frac{\pi}{2} < \beta < \frac{3\pi}{4}$ **then**
        device with position (a, b) is in the 3^{rd} sector and the device can communicate from BN_u with destination point(s,b).;
    else
        if $\frac{3\pi}{4} < \beta < \pi$ **then**
            device with position (a,b) is in the 4^{th} sector and the device can communicate from BN_l with destination point (a,t).;
        end
    end
end
if (X < 0 && Y < 0) then
$\beta \leftarrow \pi + \theta$
    if $\pi < \beta < \frac{5\pi}{4}$) then
    device with position (a, b) is in the 5^{th} sector and the device can communicate from BN_r with destination point(a,t).
    elsif ($\frac{5\pi}{4} < \beta < \frac{3\pi}{2}$) then
        device with position (a,b) is in the 6^{th} sector and the device can communicate from BN_d with destination point(s,b). **end if**
end if
if $X < 0$ && $Y < 0$ **then**
    $\beta \leftarrow \pi + \theta$;
    if $\pi < \beta < \frac{5\pi}{4}$ **then**
        device with position (a, b) is in the 5^{th} sector and the device can communicate from BN_r with destination point(a,t).;
    else
        if $\frac{5\pi}{4} < \beta < \frac{3\pi}{2}$ **then**
            device with position (a,b) is in the 6^{th} sector and the device can communicate from BN_d with destination point(s,b).;
        end
    end
end
if $X > 0$ && $Y < 0$ **then**
    $\beta \leftarrow 2\pi$ - θ;
    if $\frac{3\pi}{2} < \beta < \frac{7\pi}{4}$ **then**
        device with position (a, b) is in the 7^{th} sector and the device can communicate from BD_d with destination point(s,b).;
    else
        if $\frac{7\pi}{4} < \beta < 2\pi$ **then**
            device with position (a,b) is in the 8^{th} sector and the device can communicate from BN_r with destination point(a,t).;
        end
    end
end

α is the path loss exponent and the $\alpha \in \{2,4\}$. If the distance between the transmitter and recipient is d meter and the threshold value of the distance is d_0 then,

$$\alpha = \begin{cases} 2, & d \leq d_0 \\ 4, & d > d_0 \end{cases}$$
$$where\ d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}} \tag{7}$$

Here E_{mp} is energy cost of amplifier to transmit one bit at multi-hop model.

Using the Equation 11 in Equation 8 we get:

$$\mathbf{E_{Trans}(n, d)} = \begin{cases} E_{Embb} * n + E_{Amp} * n * d^2, & d \leq d_0 \\ E_{Embb} * n + E_{Amp} * n * d^4, & d > d_0 \end{cases}$$

The energy spent by IoT device in sleep mode is:

$$E_{sleep}(t) = E_{low} * t. \tag{8}$$

where E_{low} is the energy consumption of any device in sleep mode for one second. The total time consumed in sleep mode is t seconds.

The total energy consumed by any IoT Device in network is

$$E_{Total} = E_{Trans}(n, d) + E_{Recv}(n) + E_{sleep}(t). \tag{9}$$

V. DATA TRANSMISSION

Generally, IoT devices sense data from the environment and forward it from one to another. The process of forwarding the data continues till it reaches to the IoT hub. In this paper, we have proposed two methodologies for the transmission of data. In the first proposed methodology, the source device monitors data and forwards it to the nearest coordinating device. Further, it forwards the data to the subsequent device until it reaches the hub. In the second methodology, the source finds the IoT hub location information by connecting with the closest coordinating device and send data directly to the IoT hub.

A. PROPOSED MODEL 1

1) MOBILE IoT HUB MANAGEMENT

IoT hub moves through the network using the random way-point mobility model, and it will stop for a specific period of time (t) to gather information. IoT hub changes its location after a specific interval of time. So when it stops in a new site, it chooses a gateway device for the collection of data. This gateway device transmits the *ACK_dev* packet to the next device. The device that receives *ACK_dev* packet first time chooses the next device as the preceding device *id* as defined in algorithm 5. This process ensures until the *ACK_dev* packet reaches the coordinating device. This process is described in Figure 8. The objective here is to create a reverse link from the backbone tree device to the IoT hub.

Algorithm 5: Mobile IoT hub Management

$Gateway_s$: Gateway device chosen by s.;
$Gateway_{Chosen}$: is true when the IoT hub chooses it as the gateway device, initialized as false.;
$device_{next}$: The IoT device chooses the next device for data transmission.;
BT_a: is true when the device a is a backbone tree device, initialized as false.;
$Gateway_a$: Gateway device chosen by the device a.;
device receives the following packet from the IoT hub.;
Beacon: < Beacon, id_s>;
l_rf (BeaconReply, id_a , id_s);
The hub receives the following packets from device b.
; // BeaconReply packet is Unicasted to the IoT hub.
Beaconreply: <Beaconreply,id_b,id_s>;
if $Gateway_{chosen} == False$ **then**
  $Gateway_s \leftarrow id_b$;
  $Gateway_{chosen} \leftarrow True$;
  l_rf (Gateway, id_s , $Gateway_s$);
else
  Discard the Packet;
end
Device a receives the below packets from the IoT hub ;
Gateway: < Gateway,id_s,$Gateway_s$>;
if $id_s == Gateway_s$ **then**
  $device\_next_a \leftarrow id_s$;
  ; // As described in Algorithm 2, the gateway device selects the coordinating device and destination coordinate. The device transmits the *ACK_dev* packet to the device c nearest to the destination device using equation (14).
  l_rf (ACK_{dev}, id_a , id_c, $Gateway_s$);
else
  Discard the Packet;
end
Device a receives below packets from device b;
ACK_{dev}: <ACK_dev,id_b,id_c,$Gateway_s$>;
if $id_a == id_c$ **then**
  if $Gateway_a \neq gateway_s$ **then**
    $Gateway_a \leftarrow Gateway_s$;
    $Datasend_a \leftarrow True$;
    $dev_{next} \leftarrow id_c$;
    if $BT_a == true$ && $Parent_a == true$ **then**
      Choose the device c as parent and child id;
    else
      Select the device c nearest to the destination using equation (14);
    end
    l_rf (ACK_{dev}, id_a , id_c, $Gateway_s$);
  else
    Discard the packet.;
  end
else
  Discard the packet.;
end

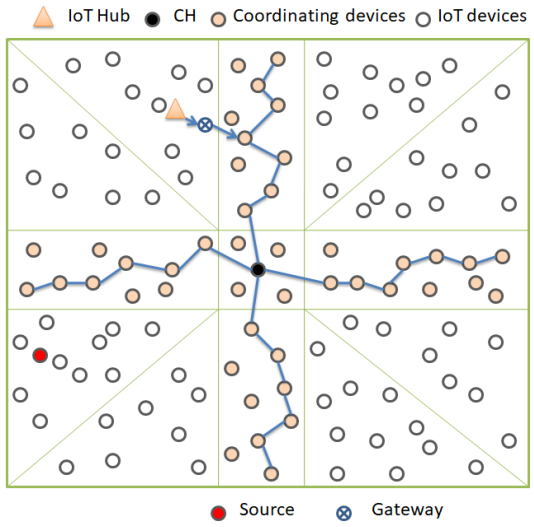

FIGURE 8. Location recovery of IoT-Hub.

2) DATA TRANSMISSION

Each IoT device has peer information, which contains peer device location and residual energy level. So the IoT device that collects the data from the environment can find a path to send data to the IoT hub as described in algorithm 5.

It sends the data packet to coordinating device through the peer devices using the *location factor* (*LF*) as shown in equation 14. *DNBR*(*j*) is the set of IoT devices which are neighbor to *j*.*LF*(*j*) is the set of location factors of each member of *DNBR*(*j*). RE_i is the residual energy state of device $i \in DNBR(j)$, (a_i,b_i) is the location information of device $i \in DNBR(j)$.

Let device *k* desires to select one of it's peer from *DNBR*(*k*) to spread the data/ control packet. Device *k* will use the *location factor* (LF) as mentioned below.

Let $x \in DNBR(i)$ with coordinates(a_x,b_x), having residual energy RE_x and let the euclidean distance of the device *x* from destination is D_x.

$$RE_{max} = \max_{x \in DNBR(i)} (RE_x) \tag{10}$$

then $LF(x)$ for x^{th} neighbor can be computed as-

$$LF(x) = RE_x * \frac{1}{D_x} = \frac{RE_x}{D_x} \tag{11}$$

where,

$$RE_x = \frac{RE_x}{RE_{max}}, \tag{12}$$

$$D_x = \sqrt{(a_{dest} - a_x)^2 + (b_{dest} - b_x)^2} \tag{13}$$

and

$$next\_device_i = max(LF(i)) \tag{14}$$

where $next\_device_i$ is the neighbor device chosen by the device *i*.

B. PROPOSED MODEL 2

1) MOBILE IoT HUB MANAGEMENT

In this proposed methodology, IoT hub informs the coordinating tree device regarding its location. Subsequently,all the coordinating tree devices will have the updated IoT hub location information, as shown in Figure 9. Anytime the IoT hub reaches to a new location it broadcasts a beacon packet.

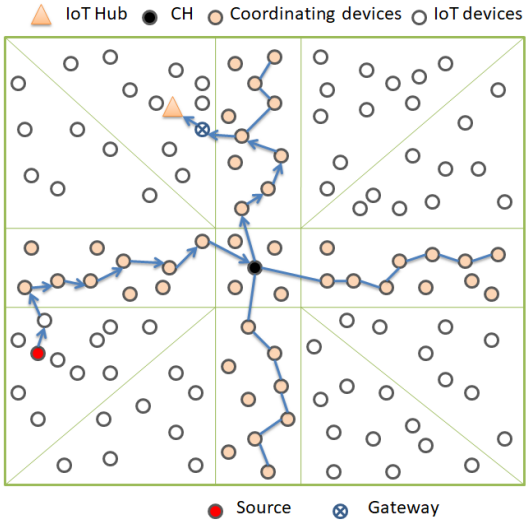

FIGURE 9. Data transmission through the tree.

This beacon packet helps to seek out the peer information of the IoT hub. As the IoT hub has it's updated peer information; it selects one of its peer device considering the minimum distance and the maximum residual energy to forward the location information as described in the algorithm 5. Again the forwarding device follows the same method to send it again. This process continues until it reaches the nearest backbone tree device. When a device in the backbone tree gets the location information, it circulates all around the tree. The communication of IoT hub management is described in algorithm 6.

2) IoT HUB LOCATION RECOVERY AND DATA TRANSMISSION

To send data, the source device required to have the coordinate location of the IoT hub. The source can get the coordinate by connecting to the nearest coordinating tree device. For this, the source broadcast a *HLoc_REQ* packet to its closest peer. The device which gets the packet forwards to nearest device. This process ensures till the *HLoc_REQ* packet approached nearest coordinating tree device. Once the coordinating tree device gets the *HL_REQ* packet, it immediately replies with its location information to the source, as shown in Figure 10. This process is described in the algorithm 7.

The process of direct data transmission initiates once the source gets the location information of the IoT hub. The source device chooses the subsequent device, with the nearest distance and most residual energy, as mentioned in equation

Algorithm 6: Mobile IoT hub Management

$IHUB\_Loc_a$: IoT hub location information stored in any device a;
BT_a : is true if any device a is a coordinating device, initialized as false;
LOC_hub: Location of the IoT hub;
Beacon: < Beacon, id_hub>;
l_rf (BeaconReply, id_a , RE_a , id_{hub}) ;
// BeaconReply packet is Unicasted to the IoT hub.
IoT hub selects the coordinating device to send it's coordinate. IoT hub sends data packet location to device c using equation (14);
l_rf (Loc, id_b, LOC_hub, $device\_next_c$) ; // data packetlocation is unicasted to the selected device c.
Device a receives the following packets from the IoT hub or any device c;
Location : < Location, id_b, LOC_hub, $device\_next_b$> ;
if $id_a == device\_next_b$ **then**
  if $IHUB\_Loc_a \neq LOC\_hub$ **then**
    IHUB_$Loc_a \leftarrow LOC_hub$;
    if $BT_a == true$ && $parent(a) == true$ **then**
      Selects device c as parent and child id;
    else
      choose device c nearest to the destination using equation (14);
    end
    l_rf (Location, id_a, LOC_hub, $device\_next_c$) ; // packetlocation is unicasted to chosen device c.
  else
    Discard the packet.;
  end
else
  Discard the packet.;
end

14. Now, the peer device can follow the same process to forward the data to the subsequent device. This remains till IoT hub gets data. The data transmission processes from source to IoT hub through intermediate devices are as shown in Figure 11.

VI. COMPLEXITY ANALYSIS OF THE PROPOSED PROTOCOL

Lemma 1: The worst-case message complexity of peer discovery process is $\mathcal{O}(\alpha)$, where α is the number of peers.

Proof: In the peer discovery process, each IoT device discovers its peer device. The device that starts the process of peer discovery broadcasts a control packet (*DNBR_CTRL*). The device receives α several control packets if it has α several peers, so the total message complexity of the peer discovery process is $\mathcal{O}(\alpha)$.

Algorithm 7: IoT hub's Location Recovery

$IHUB\_Loc_a$: IoT hub's coordinate stored in any device a;
BT_a: It is true if any device is a coordinating device;
LOC_hub: IoT hub's coordinate;
device_$next_a$: The next device chosen by any device a to forward the packet;
$LinkRev_a$: Device a selects the sender to send hub's location;
The source forward the *HUB_Loc_Req* packet to the next device using equation *LF*;
$l_rf(HUB\_Loc\_Req, id_a, device\_next_a)$; // Reply the hub position to the requesting device.
Device a receives following packets *HUB_Loc_Req*: <*HUB_Loc_req*,id_b,device_$next_b$> from any device b ∈DNBR(a);
if $id_a == device\_next_b$ **then**
  $LinkRev_a \leftarrow id_b$;
  if $BT_a == true$ && $Parent(a) == true$ **then**
    $l_rf(HUB\_Loc\_Reply, id_a, LOC\_hubLinkRev_a)$; // unicast the *HUB_Loc_Reply* packet to the next device.
  else
    The device chooses the next device using the equation 34;
    $l_rf(HUB\_Loc\_Req, id_a, device\_next)$; // send the position packet to the requested device.
  end
else
  Discard the Packet;
end
Device a receives following packet from any device b ∈DNBR(a);
HUB_Loc_reply: <*HUB_Loc_reply*,id_b,LOC_*hub*,$LinkRev_a$ >;
if $id_a == LinkRev_a$ **then**
  if $id_a == id_Source$ **then**
    $LinkRev_a \leftarrow id_b$;
  else
    $l_r(HUB\_Loc\_Reply, id_a, LOC_{hub}, LinkRev_a)$;
  end
else
  Discard the Packet;
end

Lemma 2: The cluster formation requires $\mathcal{O}(\beta\alpha)$ control messages.

Proof: Let β number of IoT devices are deployed across the network. The process of cluster formation is started by device k, which is having a high node degree which is connected to more number of peer devices and also having residual energy level more than threshold values. According to Lemma 1, the peer discovery process message complexity

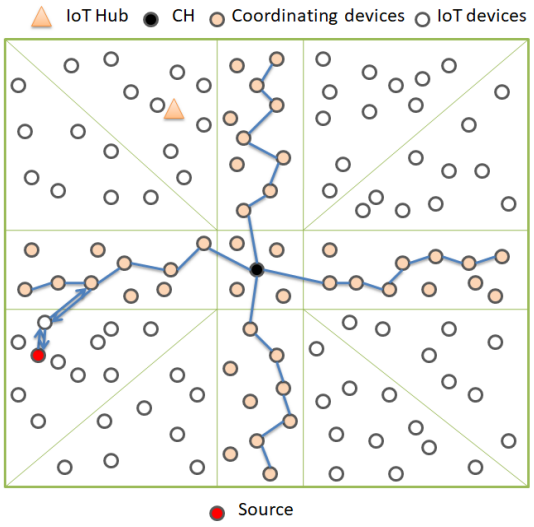

FIGURE 10. IoT-Hub location recovery.

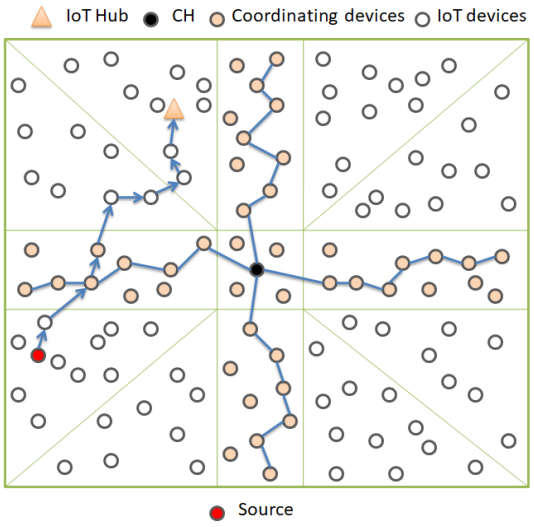

FIGURE 11. Data transmission.

of an IoT device is $\mathcal{O}(\alpha)$, where α is the number of peers. In the cluster formation process, we need to find the device z, which has the highest maximum common adjacency among the friends of the start-up device. So this process will be repeated for all β number of devices in the network. So, the message complexity for cluster formation is $\mathcal{O}(\beta\alpha)$.

Lemma 3: The total time complexity to transmit a packet from the source to the hub is $\mathcal{O}(\eta)$, where η is the number of devices present in the optimal path.

Proof: This proposed method creates a tree inside the rendezvous region by taking only the coordinating devices. So there exists an optimal path from the source to the hub. During each iteration, only one path is used for data transmission. The total path length is η if η number of devices are present across that path. Each device will forward the data that it received from the preceding device. Thus, the total time complexity to transmit a packet from the source to the hub is $\mathcal{O}(\eta)$.

Lemma 4: The total message complexity of the network is $\mathcal{O}(\beta\alpha)$.

The worst-case message complexity of the peer discovery process is $\mathcal{O}(\alpha)$, where α is the number of peers.

Proof: Let β number of IoT devices are deployed across the network. We know from Lemma 1, The worst case message complexity of the peer discovery process is $\mathcal{O}(\alpha)$, where α is the number of peers. Suppose we have used δ number of primary devices and λ number of alternate devices for the construction of the tree where $(\delta + \lambda) < \beta$. The primary device uses one broadcast message and two unicast messages, whereas alternate device uses one broadcast and one unicast message. Therefore, the total message complexity for the primary and alternate devices is $\mathcal{O}(3\delta + 2\lambda)$. The proposed routing protocol using δ number of messages for the route reply. So, the total message in the network is represented as $\mathcal{O}(\beta\ \alpha + 3\delta + 2\lambda + \delta)$. Therefore, the total message complexity of the network is $\mathcal{O}(\beta\alpha)$.

VII. SIMULATION AND RESULTS

Generally, the proposed protocol efficiency can be accessed by comparing the protocol performance on the characteristics such as the network lifetime, average energy consumption, end to end delay and packet delivery ratio with the existing protocols. We have used Castalia simulator for our simulation. It is built on the OMNET++ platform. It can be utilized to analyze different platform features for many applications. As it is highly parametric and simulate a wide range of platforms.

A. SIMULATION PARAMETER

The performance of our proposed protocol has been analyzed based on the following factors.

1) **Control packet overhead:**
Control packets are the packets which are used for path construction, peer discovery, cluster formation, maintenance process, etc. These are not data packets, so energy consumed by IoT devices for transmission and reception of control packets is known as control packet overhead.
2) **End-to-end latency:**
A better routing protocol should be robust. The robustness is hampered due to the delays present in the network. The different types of delays present in the network are queuing delay, route discovery delay, and processing delay. Hence, the time taken by the network for data packet transmission from source to IoT hub is the end to end latency.
3) **Energy consumption:**
The efficiency of the routing protocol relies on energy consumption. The less the network energy consumption, the more the network lifetime. Therefore, it is the total energy consumed by IoT devices to

TABLE 3. Simulation parameter.

Simulation Parameters	values
Simulator	Castalia Simulator (version 3.2)
Number of IoT devices	200
Initial energy of devices	20J
IoT Sensing Network area	$100*100m^2$
IoT-Hub speed	(5, 10, 15, 20, 25) m/sec
Simulation time	200s
Mobility model	Gauss Mobility model
MAC protocol	Tunable Mac

perform transmission, reception, listening, processing, and sleeping activities.

4) **Packet delivery ratio:**
A better routing protocol ought to be reliable. The reliability relies upon the ratio; more the packet delivery ratio, better is the reliability. It is defined as the ratio of IoT hub receipt data packets to data packets sent by the source.

5) **Network lifetime:**
It is the time duration where the network works perfectly. The definition of network lifetime varies from application to application. For a few applications, it is the time duration until the first IoT device dies or a percent of IoT devices die. In this paper, we have improved the network lifetime as it depends upon the energy spent by the IoT devices. Here we have reduced the energy needed for different activities like peer discovery, route establishment, maintenance, and data transmission.

We have compared the result with exiting highly cited protocols like LBDD routing protocol [30], RRP1 (Ring Routing Protocol) [33] and RRP2 (Railroad Routing Protocol) [34]. While performing experiments, the speed of the hub was varied from 5 to 25 m/s. We perceived the impact of varying hub speed on data delivery ratio, energy consumption, and end-to-end latency. Table 1 contains the simulation parameters.

B. AVERAGE CONTROL PACKET OVERHEAD

It is a sensor device which transmits the control packets for construction of the rendezvous zone and managing the mobility of IoT hub. Figure 12 illustrates the average energy consumption of the control packet when hub speed is varied in different protocols. The control packet overhead is less in the proposed methodology two as compared to other protocols, as shown in the graph.

In LBDD, the task of the inline device is to store the data received from the sensor device. Whenever the inline device gets a query, it forwards the data to the hub. The query sent by the hub is flooded into the rendezvous zone. So the control packet overhead is increased. The station formation and construction of the rail is a one time process in railroad protocol. But the process involved meta data storage and retrieval of the location of the hub, which involves

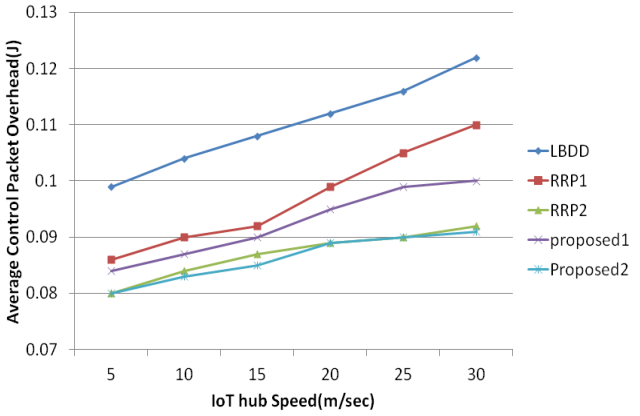

FIGURE 12. Control packet overhead.

an exchange of control packets. The ring devices store the location information of the hub. It makes the easy extraction of the hub location. As the network operation progresses, the exchange of control packets is essential for repairing the ring. The distance between the source and hub increases with the rise of ring length, which leads to additional energy consumption.

Control packet overhead in the first proposed methodology, is more as it requires more control packets to form the multi-path in the rendezvous zone and a cluster in the intersection of the cross areas. But in the second proposed methodology, the distance between the source and hub reduces. So less no of control packets are required for data transmission.

C. AVERAGE ENERGY CONSUMPTION

Figure 13 illustrates total energy consumption with numerous protocols. It was ascertained that the energy consumed in LBDD was highest owing to greater control packet overhead. Data from the source device is stored there, and the hub query is flooded within the rendezvous zone. With the rise in hub speed, energy consumption is accrued monotonically.

In the first proposed methodology, the hub location is not needed for data transmission. The average distance between the source and hub is more as compared to rail and ring routing protocol as the source always communicates to the hub through the rendezvous region. Hence, the energy consumption increases with the increasing hub speed. In the second proposed methodology, the average distance from source and hub is the same as rail and ring routing. However, in the second proposed methodology, the average control packet requirement is less. So it performs better as compared to others.

D. END TO END LATENCY

The latency of various protocols with a varying speed of hub is shown in Figure 14. This will rely upon the time taken to seek out the hub location and spread data to the hub.

In the first proposed methodology, whenever the sink changes its position, it got upgraded to a new position to

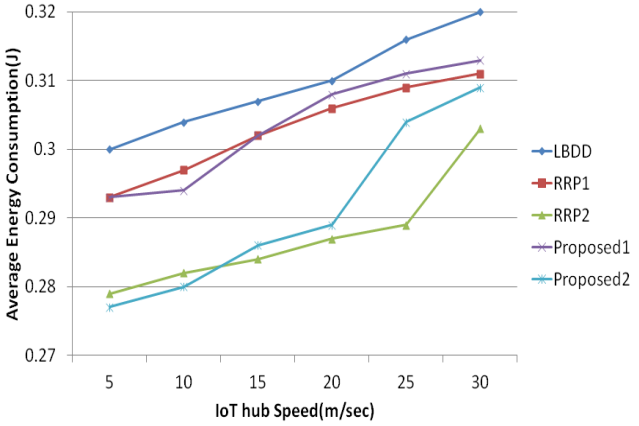

FIGURE 13. Average energy consumption.

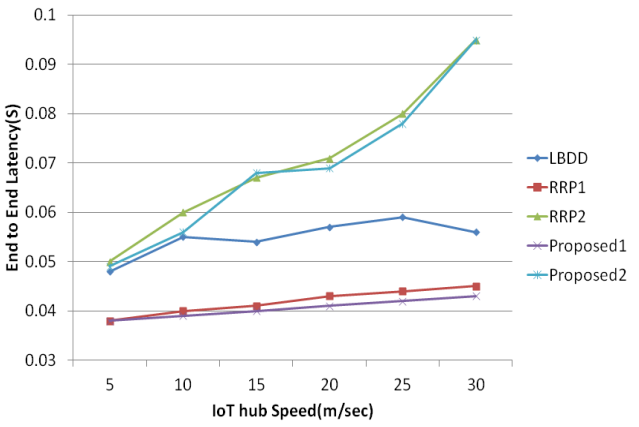

FIGURE 14. End to end latency.

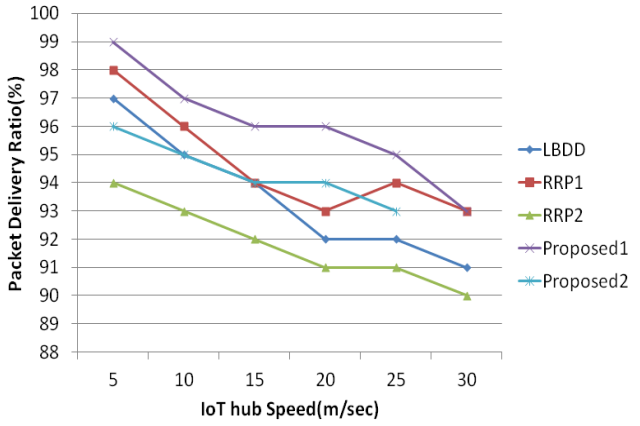

FIGURE 15. Packet delivery ratio.

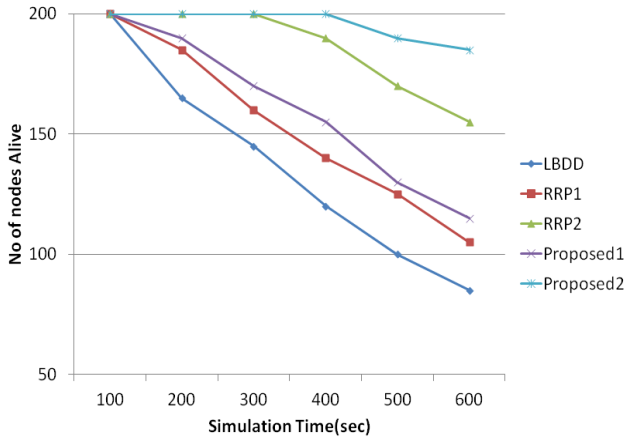

FIGURE 16. Network lifetime.

the coordinating device. Therefore, a reverse route is established. Hence, whenever the source sends any data packet, it requires to send the data packet only to the nearest coordinating device. As the route has been established previously, the delay reduces. If any device in the tree dies, a new path establishes immediately, which helps to reduce the delay. However, in LBDD, as it needs the hub location, the delay increases. But In the second proposed methodology, the delay is less as compared to Rail and Ring protocols. As the division of network plane to sectors helps reduce the communication time. As a result, delay reduces.

E. PACKET DELIVERY RATIO

The packet delivery ratio of various protocols is shown in Figure 15. In this, the rate of success of the data received at the hub is shown.

In the first methodology of data transmission, there is a dynamic path between the source and hub through the coordinating devices. As we have got established a multipath, therefore the failure of any device within the tree won't cause any data loss. Hence, the packet delivery ratio is greater as compared to others. In LBDD, finding the hub locations are required by the source to send data. Thus, each time, the source needs the hub location to establish a route that will increase the possibility of data loss. In Rail as well as Ring protocol, the time necessary to seek out the hub location is more as compared to the second proposed methodology. Thus, whenever the hub changes its position, the source won't get the new location of the hub immediately, which increases the data loss.

F. NETWORK LIFETIME

The lifetime of the network depends on the energy consumed at each device and imbalance in load among the sensor devices. As illustrated in Figure 16, the network lifetime is increased in the second proposed methodology as compared to other protocols. It is due to the less number of control packets, load balancing among the device and choice of the optimal route for data transmission.

VIII. CONCLUSION

In this research paper, a rendezvous-based routing protocol is proposed where a rendezvous region is constructed inside the network. Further, a primary and alternate path is also built

within this region. In the protocol, we have proposed two methods for transmission of data.

In the first proposed methodology, the source will send the data packet to the nearest coordinating device; further, the data packet will move till it reaches the hub. Also, we have established a reverse route from the hub previously. In the second proposed methodology, the source only retrieves the hub location by connecting with the coordinating device and data packets being sent directly towards the hub through the intermediate devices.

The two methodologies proposed were compared with protocols that already exist like LBDD, rail routing, and ring routing. Based on results obtained from simulation, it has been observed that the proposed first method beats the present protocols in parameters like end-to-end latency and delivery ratio. The energy consumed by the proposed second method is very less when compared with that of the present protocols.

However, due to the random deployment of the sensor devices in remote areas, these WSN assisted IoT networks are vulnerable to numerous security threats that can adversely affect the network performance. So there is a need for an energy-efficient, secure routing protocol that requires low power and computing cost. Further, future work may reduce the complexity of the proposed sensing framework and explore its implementation in real-time.

REFERENCES

[1] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, May 2016.
[2] M. Hammoudeh, F. Al-Fayez, H. Lloyd, R. Newman, B. Adebisi, A. Bounceur, and A. Abuarqoub, "A wireless sensor network border monitoring system: Deployment issues and routing protocols," *IEEE Sensors J.*, vol. 17, no. 8, pp. 2572–2582, Apr. 2017.
[3] C. Cimen, E. Cayirci, and V. Coskun, "Querying sensor fields by using quadtree based dynamic clusters and task sets," in *Proc. IEEE Mil. Commun. Conf. MILCOM*, vol. 1, Oct. 2003, pp. 561–566.
[4] R. Chaudhry, S. Tapaswi, and N. Kumar, "A green multicast routing algorithm for smart sensor networks in disaster management," in *Proc. IEEE Trans. Green Commun. Netw.*, vol. 3, no. 1, pp. 215–226, Mar. 2019.
[5] N. Kumar and D. P. Vidyarthi, "A green routing algorithm for IoT-enabled software defined wireless sensor network," *IEEE Sensors J.*, vol. 18, no. 22, pp. 9449–9460, Nov. 2018.
[6] F. K. Shaikh, S. Zeadally, and E. Exposito, "Enabling technologies for green Internet of Things," *IEEE Syst. J.*, vol. 11, no. 2, pp. 983–994, Jun. 2017.
[7] C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.
[8] R. Arshad, S. Zahoor, M. A. Shah, A. Wahid, and H. Yu, "Green IoT: An investigation on energy saving practices for 2020 and beyond," *IEEE Access*, vol. 5, pp. 15667–15681, 2017.
[9] T. H. Szymanski, "Security and privacy for a green Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 34–41, Oct. 2017.
[10] X. Liu and N. Ansari, "Toward green IoT: Energy solutions and key challenges," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 104–110, Mar. 2019.
[11] R. K. Lenka, A. K. Rath, Z. Tan, S. Sharma, D. Puthal, N. V. R. Simha, M. Prasad, R. Raja, and S. S. Tripathi, "Building scalable cyber-physical-social networking infrastructure using IoT and low power sensors," *IEEE Access*, vol. 6, pp. 30162–30173, 2018.
[12] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: A top-down survey," *Comput. Netw.*, vol. 67, pp. 104–122, Jul. 2014.
[13] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. D. Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1417–1425, May 2014.
[14] T. D. Nguyen, J. Y. Khan, and D. T. Ngo, "A distributed energy-harvesting-aware routing algorithm for heterogeneous IoT networks," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 4, pp. 1115–1127, Dec. 2018.
[15] S. Roy, D. Puthal, S. Sharma, S. P. Mohanty, and A. Y. Zomaya, "Building a sustainable Internet of Things: Energy-efficient routing using low-power sensors will meet the need," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 42–49, Mar. 2018.
[16] R. C. Shit, S. Sharma, D. Puthal, and A. Y. Zomaya, "Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2028–2061, 3rd Quart., 2018.
[17] B. Spinelli, L. E. Celis, and P. Thiran, "A general framework for sensor placement in source localization," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 2, pp. 86–102, Apr./Jun. 2019.
[18] C. Tunca, S. Isik, M. Y. Donmez, and C. Ersoy, "Distributed mobile sink routing for wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 877–897, 2nd Quart., 2014.
[19] L. Mottola and G. P. Picco, "MUSTER: Adaptive energy-aware multi-sink routing in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 12, pp. 1694–1709, Dec. 2011.
[20] Z. Han, J. Wu, J. Zhang, L. Liu, and K. Tian, "A general self-organized tree-based energy-balance routing protocol for wireless sensor network," *IEEE Trans. Nucl. Sci.*, vol. 61, no. 2, pp. 732–740, Apr. 2014.
[21] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 788–800, Apr. 2016.
[22] H.-H. Liu, J.-J. Su, and C.-F. Chou, "On energy-efficient straight-line routing protocol for wireless sensor networks," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2374–2382, Dec. 2017.
[23] S. Sharma, D. Puthal, S. Tazeen, M. Prasad, and A. Y. Zomaya, "MSGR: A mode-switched grid-based sustainable routing protocol for wireless sensor networks," *IEEE Access*, vol. 5, pp. 19864–19875, 2017.
[24] A. Salim, W. Osamy, and Ahmed M. Khedr, "IBLEACH: Intra-balanced LEACH protocol for wireless sensor networks," *Wireless Netw.*, vol. 20, no. 6, pp. 1515–1525, Aug. 2014.
[25] D. Zhang, G. Li, K. Zheng, and X. Ming, "An energy-balanced routing method based on forward-aware factor for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 766–773, Feb. 2014.
[26] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *Proc. Euro Med Telco Conf. (EMTC)*, Nov. 2014, pp. 1–5.
[27] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.
[28] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, "A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.
[29] M. Elshrkawey, M. Samiha Elsherif, and M. ElsayedWahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 30, no. 2, pp. 259–267, Apr. 2018.
[30] E. B. Hamida and G. Chelius, "A line-based data dissemination protocol for wireless sensor networks with mobile sink," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 2201–2205.
[31] S. Sharma, D. Puthal, S. K. Jena, A. Y. Zomaya, and R. Ranjan, "Rendezvous based routing protocol for wireless sensor networks with mobile sink," *J. Supercomput.*, vol. 73, no. 3, pp. 1168–1188, Mar. 2017.
[32] X. Liu, "Atypical hierarchical routing protocols for wireless sensor networks: A review," *IEEE Sensors J.*, vol. 15, no. 10, pp. 5372–5383, Oct. 2015.
[33] C. Tunca, S. Isik, M. Y. Donmez, and C. Ersoy, "Ring routing: An energy-efficient routing protocol for wireless sensor networks with a mobile sink," *IEEE Trans. Mobile Comput.*, vol. 14, no. 9, pp. 1947–1960, Sep. 2015.
[34] J.-H. Shin, J. Kim, K. Park, and D. Park, "Railroad: Virtual infrastructure for data dissemination in wireless sensor networks," in *Proc. 2nd ACM Int. Workshop Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw.*, Oct. 2005, pp. 168–174.
[35] Z. Hameed and Y.-B. Ko, "A quadtree-based data dissemination protocol for wireless sensor networks with mobile sinks," in *Proc. IFIP Int. Conf. Pers. Wireless Commun.*, Berlin, Germany: Springer, 2006, pp. 447–458.
[36] J. Shen, A. Wang, C. Wang, P. C. K. Hung, and C.-F. Lai, "An efficient centroid-based routing protocol for energy management in WSN-assisted IoT," *IEEE Access*, vol. 5, pp. 18469–18479, Sep. 2017.

[37] N. D. Tan and N. D. Viet, "SCBC: Sector-chain based clustering routing protocol for energy efficiency in heterogeneous wireless sensor network," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2015, pp. 314–319.

RAKESH KUMAR LENKA is currently pursuing the Ph.D. degree with the Veer Surendra Sai University of Technology (VSSUT), Burla. He is also an Assistant Professor with the Department of Computer Science and Engineering, International Institute of Information Technology (IIIT) Bhubaneswar. He has published over 35 research articles in his name in reputed journals and conference proceedings. His research interests include fog/mist computing, the IoT sensing infrastructure deployment, DFA-based pattern matching, recommendation systems, geographical information systems, and sensor networks. He is a Professional Member of the CSI and the International Association of Engineers (IAENG). He has served as a Reviewer for various reputed international journals and conferences.

AMIYA KUMAR RATH received the B.E. degree in computer science from Marathwada University, Maharastra, in 1990, the M.B.A. degree in systems management from Shivaji University, in 1993, the M.Tech. degree in computer science from Utkal University, in 2001, and the Ph.D. degree in computer science from Utkal University, in 2005, with a focus on embedded system. He is currently a Professor with the Department of Computer Science and Engineering, Veer Surendra Sai University of Technology (VSSUT), Burla, India. He is also deputed to the National Assessment and Accreditation Council (NAAC), Bengaluru, India. He has contributed more than 80 research-level articles to many national and international journals and conferences. He has published seven books by reputed publishers. His research interests include embedded systems, ad hoc networks, sensor networks, power minimization, evolutionary computation, and data mining.

SURAJ SHARMA received the Ph.D. degree from the National Institute of Technology Rourkela, India. He is currently an Assistant Professor with the Department of Computer Science and Engineering, International Institute of Information Technology Bhubaneswar, Bhubaneswar. His research interests include the Internet of Things (IoT), wireless sensor networks, and information security.