IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CYBER-PHYSICAL-SOCIAL COMPUTING AND NETWORKING

Received April 17, 2018, accepted May 15, 2018, date of publication June 1, 2018, date of current version June 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2842760

Building Scalable Cyber-Physical-Social Networking Infrastructure Using IoT and Low Power Sensors

RAKESH KUMAR LENKA[1], AMIYA KUMAR RATH[2], ZHIYUAN TAN[3], SURAJ SHARMA[1], DEEPAK PUTHAL[4], N. V. R. SIMHA[1], MUKESH PRASAD[4], ROHIT RAJA[5], AND SHANKAR SHARAN TRIPATHI[6]

[1]Department of Computer Science and Engineering, International Institute of Information Technology at Bhubaneswar, Bhubaneswar 751003, India
[2]Department of Computer Science and Engineering, Veer Surendra Sai University of Technology, Burla 768018, India
[3]School of Computing, Edinburgh Napier University, Edinburgh EH14 1DJ, U.K.
[4]Faculty of Engineering and IT, University of Technology Sydney, Ultimo, NSW 2007, Australia
[5]CSE Department, Sreyas Institute of Engineering and Technology, Hyderabad 500068, India
[6]Department of Computer Science and Engineering, Shri Shankaracharya College of Engineering and Technology, Bhilai 491001, India

Corresponding authors: Zhiyuan Tan (z.tan@napier.ac.uk) and Deepak Puthal (deepak.puthal@uts.edu.au)

ABSTRACT Wireless sensors are an important component to develop the Internet of Things (IoT) Sensing infrastructure. There are enormous numbers of sensors connected with each other to form a network (well known as wireless sensor networks) to complete the IoT Infrastructure. These deployed wireless sensors are with limited energy and processing capabilities. The IoT infrastructure becomes a key factor to building cyber-physical-social networking infrastructure, where all these sensing devices transmit data toward the cloud data center. Data routing toward cloud data center using such low power sensor is still a challenging task. In order to prolong the lifetime of the IoT sensing infrastructure and building scalable cyber infrastructure, there is the requirement of sensing optimization and energy efficient data routing. Toward addressing these issues of IoT sensing, this paper proposes a novel rendezvous data routing protocol for low-power sensors. The proposed method divides the sensing area into a number of clusters to lessen the energy consumption with data accumulation and aggregation. As a result, there will be less amount of data stream to the network. Another major reason to select cluster-based data routing is to reduce the control overhead. Finally, the simulation of the proposed method is done in the Castalia simulator to observe the performance. It has been concluded that the proposed method is energy efficient and it prolongs the networks lifetime for scalable IoT infrastructure.

INDEX TERMS Internet of Things, wireless sensor network, WSN-assisted IoT, area-based routing, hot spot problem, routing protocol.

I. INTRODUCTION

IoT comprises of huge sum of devices (sensors) that are connected with each other leading to form a Wireless Sensor Network (WSN). On the other hand WSN is a network [1] that consist of huge number of sensor nodes that observe the environmental phenomenon and transform collected data into signals. In general, IoT can be defined as the competence to communicate and connect remotely to manage several networked automated devices via internet [23]. A device in IoT environment can be defined as a ''device or a thing'' with computational intelligence embedded in it and can connect to a network. These devices are cost-effective, optimized in power consumption and intelligent systems. IoT predictors estimated that there will be more than 100 Billion devices will be connected to internet by 2020 [22], [24]. This number doesn't include general internet devices like computers, tablets and smartphones, but includes those devices that can indirectly have a connection to the internet (like sensors nodes) [25], [26]. Wireless Sensor Networks (WSN) are a major part of the Internet of Things. It can also treat as a bridge to connect the digital world with the real world. Which took responsibilities for passing the real world sensed information to the Internet embedded electronics, actuators, sensors, software, and so on [33]–[35]. The IoT architecture has been shown in Figure 1. The technology of WSN-assisted IoT can be extended to use in a wide range of application

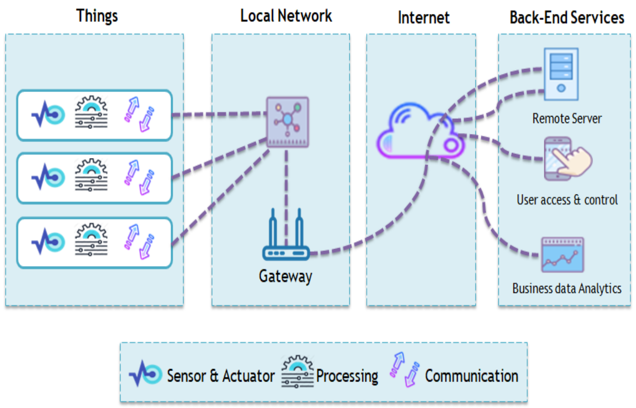

FIGURE 1. IoT Architecture.

starting from the armed forces, traffic monitoring, intelligent building [36]–[38], intelligent transportation system, civilian domains and other fields [39], [40], [44].

As these sensor networks grow in size, they encompass a large amount of data. This huge amount of data spread across the whole network, which requires the use of data dissemination techniques. The data dissemination techniques can extract data relevant to the user and make it available. Dissemination of data is the method to allocate requests sent by the user and data collected among the devices [17]. WSN-Assisted IoT can be used for gathering data with the help of cloud computing [41], [42], [45]. IoT-Hub is used to connect, monitor and manage billions of IoT assets. IoT-Hub can establish reliable, bi-directional communication with IoT devices (Sensor Nodes). It can gather real-time data from the IoT devices and upload files to the cloud. Data is transmitted either directly or through the intermediate devices. The IoT-Devices have to search the path up to the IoT-Hub for data transmission. Though the IoT hardware capabilities are increasing, the battery capacity of the devices is not increasing at the same rate [28]. IoT devices have limited-power batteries which are not rechargeable. As mostly, they are deployed in a difficult terrain, these batteries cannot be replaced easily. Without the use of advanced power saving schemes and overall reduced energy consumption, it is not favorable to adopt IoT technologies [23], [27], [29]. As these IoT devices are energy-constrained and are equipped with limited memory and computing power, energy efficient routing protocols are required to route the data towards the IoT-Hub. Also, it is extremely difficult to provide global IDs to the IoT devices. Routing protocols should have proper resource management techniques to prolong the network lifetime and make it fault tolerant and robust. Due to these challenges, many new protocols have been proposed in recent years [2]–[4], that eliminate the energy inefficiencies that are shortening the lifetime of the network.

One of the crucial issues in WSN-Assisted IoT Networks is the Hot Spot problem. The IoT devices closer to the IoT-Hub drain their energy at a faster rate compared to other IoT devices as they have to perform more communication and hence the WSN-Assisted IoT network may get detached or isolated [21], [30]–[32]. It is very difficult to recharge or replace the battery of these IoT devices in the middle of the operation. So we must use the energy of the IoT devices in an efficient way, hence they last longer [18], [19]. IoT devices mainly loses their energy while transferring and receiving the data from other devices. For this purpose, we should use efficient data routing techniques so that while sensing or transmitting the data, much energy is not being consumed [11]–[13]. If the energy consumption of IoT devices is reduced, then this will lead to increased network lifetime.

For the purpose of less energy consumption, we can consider many techniques such as clustering technique, using the intermediate IoT devices for sending the data, using efficient routing protocols for data reception and transmission etc [20], [43]. Generally IoT devices are deployed in a random manner in the region. Now these IoT devices will sense the environment and transmit the data to the IoT-Hub. As these IoT devices are deployed randomly, if a IoT Device, located at a farther distance from the IoT-Hub and wants to send the data, then it has to send data directly to IoT-Hub in the general scenario which will cause more energy consumption [14]–[16]. The device may die early leading to the reduced network lifetime. If they use intermediate IoT devices to send the data, then there is a chance of less energy consumption.

In this paper, we have discussed some of the routing protocols applicable to WSN-Assisted IoT Networks. These protocols provide better scalability and efficient communication among the Devices. In cluster based routing techniques, Devices are organized in a hierarchy where some of the IoT devices play the role of high-tier IoT devices which transmit and receive the data while some IoT devices are low tier IoT devices that sense the data. Basically, cluster formation occurs in the network among IoT devices and two-layer routing is performed. In the first layer, it elects the cluster head and the second layer is used for routing. The cluster-based routing protocols are subdivided into area-based routing, location-based routing, grid-based routing and chain-based routing. The area-based routing protocols divide the network into different region in which some of the Devices act as high-tier IoT devices while other are low-tier IoT devices. Basically, cluster formation occurs in the network among devices and two layer routing is performed. The identity of the devices can be determined by noticing the region to which they belong. After the literature survey, a rendezvous routing protocol in cluster-based model is proposed in this paper. We have used the concepts of rendezvous routing [8] and LBDD protocols [5] as a reference. In this paper, we have implemented the proposed protocol using IoT sensor devices.

II. RELATED WORK

In recent years, many area-based routing protocols for WSN and WSN-Assisted IoT Networks have been proposed. Some of the recent works are discussed in the next section.

LBDD routing protocol [5] defines a wide vertical strip of devices horizontally centered on the area of deployment. This can also be segregated into sets of size g. Those devices which lie in this virtual infrastructure are termed as inline devices. Device's data are sent to the line and the first inline device encountered stores the data. Data Dissemination: When an IoT device (sensor) senses some data, it transfers that data to the nearest inline device. Data Collection: When an IoT-Hub requires data it sends a request to virtual route in a vertical manner. The aligned device first sends it in both directions along the path with line. When the query reached out to relevant data containing IoT device, then that IoT device will directly send the data to the IoT-Hub. Sometimes it may happen that numbers of the query are higher than the data. LBDD relies on broadcasts for propagating data queries along the line. The line structure can be established very easily with low overhead. This line has to be wide enough to mitigate hot-spots problem. It decreases the energy consumption and increases the overhead.

Ring Routing protocol forms a ring-like structure or a closed loop which divides the network into some rendezvous area [6]. After the deployment of the network, first of all, an initial radius is determined. Those devices that are the part of this ring structure are selected and termed as ring devices. Ring devices help regular devices on getting the information about the IoT-Hub's updated position. Initially, the device closest to the IoT-Hub is chosen as Anchor Node (AN). On selecting anchor node, IoT-Hub broadcast Anchor Selection (ANS) packet. After selecting a new AN, it sends an Anchor Node Position Information (ANPI) packets towards the ring. The nodes in the ring share information with neighbors upon receiving the ANPI packet. The source device sends the AN Position Information Request packet (ANPIREQ) towards the ring. On receiving the request, the ring devices sends the AN Position Information Response (ANPIRES) packet that contains current AN's position information to the source. On receiving the response packet from the ring node, the source can now send the data towards the AN. Ring Routing protocol reduces the control packets by incorporating the minimum number of nodes to be in the ring. Ring Routing works with minimal inefficient broadcasts, those are widely used in area-based protocols.

The Railroad protocol exploits the rail infrastructure [7] where all the meta-data of event data are stored. The devices in the rail are called rail devices. When the IoT device senses some data, then it forwards the corresponding meta data to the nearest station, which is a group of rail devices. The devices in the station are called platform devices. The process of construction of rail occurs only once at the time of set up stage. To determine whether a device is in rail it should know its distance from the nearest boundary device and network center. Event notification message alerts the rail about the summary of the event. Once the rail device receives the message, it forms the new station and passes the message to the platform devices in the station. The Railroad is different from LBDD by introducing a key factor, i.e. the IoT-Hubs queries go with unicast rather than broadcast by traveling on the rail. In order to encounter a device with meta-data from the query, stations should cover the rail width. Finally, delaying the data delivery in Railroad protocol is comparatively higher than LBDD, as the query cover the longer distance.

To retrieve the information IoT-Hub issues a query. This query is forwarded to source in three phases. Query forwarding on the rail, circulation of query around the rail, query notification to the source. IoT-Hub sends the query to its neighbor device and then devices in the path forward it towards the rail. Once the query enters in the rail it circulates around with the help of directional information. It also examines all the station in mid of its trip. If any station has relevant data that IoT-Hub requires then platform device sends query notification message to the source. After receiving the query notification message, the source sends the data to the IoT-Hub.

In Virtual cross area routing protocol [8] a virtual crossover the region of width w, consisting of horizontal and vertical regions, is constructed which resides in the middle of the network. This virtual structure divides the network into four parts 1- horizontal left, 2- horizontal right, 3-vertical up, 4-vertical bottom. This cross area acts as a rendezvous area. Devices in this cross area are called as backbone devices. A tree will be constructed in this area and some of the backbone devices are the part of the tree. This tree is responsible for sending the information from the source to IoT-Hub and from IoT-Hub to the source. The devices which take part in tree construction knows the IoT-Hub position but other backbone devices do not have any information regarding the IoT-Hub position.

In Quadtree-based routing protocol (QDD) [9] space partitioning is done by exploiting quadtree structure in the network. This protocol is designed based on the following assumptions:

IoT devices are static and know their location, they also have knowledge about their one-hop neighbors whereas all the stimuli and IoT-Hub is mobile. IoT devices known the complete area of WSN-Assisted IoT network, i.e. N, defined as $2^m \times 2^m$; where m $= log_2$ (N). For data and packet dissemination this protocol uses greedy forwarding algorithm. In comparison with other existing hierarchical approach, construction quad-tree structure in QDD is minimal. But there is also a loop falls, where QDD is not addressing the hot-spot problem.

The Centroid-Based Routing Protocol (CBRP) [33] proposed an energy-efficient data routing protocol for the Internet of Things using a sensor device to improve the overall network performance. In this, the clustering has been done by the Base Station (BS) based on the distances from the BS. It maintains a uniform distribution of energy in the cluster by founding Candidate Cluster Head (CH) device. The BS takes the responsibility of cluster formation which helps in reducing cluster formation overhead. It uses a threshold distance to transmit the data packets. If the distance is more than the threshold, then data loss occurs. The process of reelections of cluster head has not been defined.

The Sector-Chain Based Clustering Routing Protocol (SCBC) [10] divides the entire WSN-Assisted IoT network area into sectors (cluster). It constructs chain for each cluster with the chain leader as the cluster head (CH) and secondary cluster head (SCH) that has high residual energy. The SCH has the shortest distance between candidate nodes and the base station (BS) in the network. It reduces energy dissipation of the network by using chains for data transmission. The SCH is used to reduce energy consumption over CH. The Base Station (BS) forms the clusters and selects the cluster head, which results in the consumption of more energy for further rounds.

For the table 1, we consider that H as High, L as low, M as Moderate, VL as Very low.

TABLE 1. Comparison of different area-based protocols in WSNs.

Protocols	Control packet overhead	Energy consumption	End to End delay	Packet delivery ratio	Network life time
LBDD	H	H	L	M	M
Ring routing	L	L	L	H	H
Railroad	M	M	M	H	M
Virtual cross area	VL	M	L	L	M
Quadtree	M	M	M	L	L
CBRP	M	L	M	H	M
SCBC	M	M	M	H	M

III. PROPOSED WORK

In the proposed data routing protocol, IoT network consists of several static IoT devices, say n and a mobile IoT-Hub (sink) (for reducing the hot spot problem). IoT Network infrastructure is partitioned by cross area and clusters are constructed inside it. The IoT-Hub send its updated position information to devices inside the cross area and source IoT device takes IoT-Hub's current location information from the devices residing in the cross area and sends data to IoT-Hub. A virtual infrastructure region of horizontal and vertical width w is created at the center of the IoT network infrastructure. The IoT devices are static in nature as shown in Figure 2. The network is partitioned by the cross area and clusters are constructed inside it as shown in Figure 3.

This virtual structure divides the network into four parts: 1. Horizontal left H_l, 2. Horizontal right H_r, 3. Vertical up V_u, 4. Vertical bottom V_b. This cross area act as a rendezvous area as shown in Figure 3. The IoT devices which are within this rendezvous area are termed as the coordinating devices (backbone nodes). In this cross area, clusters are constructed based on node degree and maximum common adjacency. Each cluster consists of one cluster head. These cluster heads are responsible for sending the IoT-Hub's position to the source devices and updating the IoT-Hub position according to the present location of IoT-Hub. This protocol composed of many phases such as neighbor discovery, forming a cross area, cluster formation, cluster head selection, discovering IoT-Hub location and finally transmission of data.

Algorithm 1 Neighbor Discovery

$Nb(m)$ Set of neighbors of any device m initialized to ϕ.
$Nb_{table}(m)$: Neighbor table maintains by device m initialized to ϕ
E_{r_m}: Energy of device m.
NBR_D_m: Neighbor discovery control packet of device m sets true if sensor device m sends the packet. Initialized to false.
Loc_m: location of device m.
device n sends NBR_D packet to device m
NBR_D: $<$ NBR_D, id_n ,Er_n, Loc_n $>$
if ($id_n \notin$ Nb(m)) **then**
Nb(m)= Nb(m) $\bigcup$ n;
Update Nb_{table}(m) with $< id_n, Er_n, Loc_n >$
    if (NBR_D_m == false)
    then
    NBR_$D_m \leftarrow$ true
    l_rb(NBR_D_m, id_m , Er_m , Loc_m);
        ▷ Broadcast the NBR_D packet
    else Discard the packet
    endif
else Discard the packet
endif

A. ASSUMPTIONS

1) After the deployment, all IoT devices are stationary.
2) IoT-Hub will change its position, i.e. IoT-Hub is mobile.
3) There is no limitation of computation power, battery consumption and memory for IoT-Hub.
4) But the IoT devices has limited energy, computational capability and memory.
5) All the IoT devices are homogeneous.
6) Each device is assigned a unique Local ID.

B. NEIGHBOR DISCOVERY

In this phase, each IoT devices finds its neighbor devices. In the first phase of neighbor discovery, IoT devices broadcast the Neighbor Discovery (*NBR_D*) control packet that contains the ID of the device, the device location and its residual energy level.

On receiving this packet the device maintains the neighbor table that contains the device ID of the sender, it's position (location) and remaining energy level. If there is already an entry of the sender devices in the neighbor table, then the packet is discarded by the receiver. The receiver also broadcasts the *NBR_D* packet once if it was not broadcasted previously. At the end of this phase, all IoT devices have the information about their one hop neighbors.

C. CROSS AREA FORMATION

A cross strip acts as a rendezvous area in the IoT network and to construct it, the maximum sensing network area should be

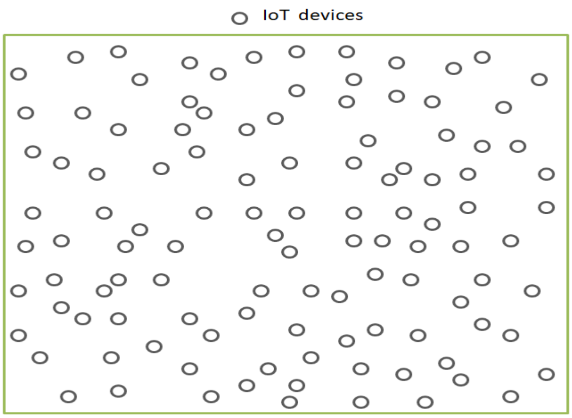

FIGURE 2. Initial view of sensor area.

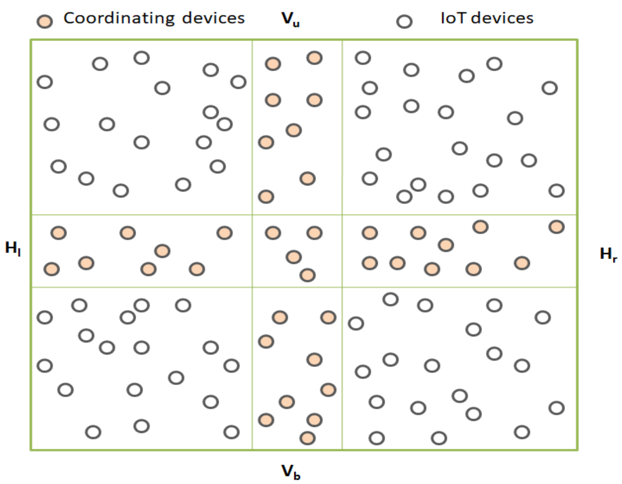

FIGURE 3. Rendezvous area with backbone nodes.

known. Let us consider the maximum sensing network area is (M_{max},N_{max}) and the width of the strip as w. So w_x and w_y the horizontal and vertical range of the strip can be defined as-

$$w_x = (M_{max} - w)/2 \quad to \quad (M_{max} + w)/2 \tag{1}$$
$$w_y = (N_{max} - w)/2 \quad to \quad (N_{max} + w)/2 \tag{2}$$

D. REGION DISCOVERY OF IoT DEVICES

The IoT devices use their location information coordinates (x, y) to determine the octant in which they belong. For instance, the IoT devices that are residing in first and eighth octant will communicate from H_r with target position (x_i,v). In the same manner, second and third octant IoT devices can communicate from V_u with target position (u, y_i) where (u, v) is the center of the network. Figure 4 shows the region discovery for IoT devices.

E. CLUSTER FORMATION

Clusters are built inside the rendezvous area by following steps:

Algorithm 2 Region Discovery for IoT Devices

θ=0,α=0
(u,v): center of the network
(x_i, y_i): location of a device
Let $\pi = 180°$; C ← (u,v)
▷ C_n defines the center of the WSN-Assisted IoT network.
Calculate new coordinates (x_i-u, y_i-v) of device x with location (x,y)
(P, Q) ← (x_i-u,y_i-v)
Now find $\theta = tan^{-1} \mid \frac{Q}{P} \mid$
if (P > 0 && Q> 0) **then**
$\alpha \leftarrow \theta$
if(α is in between 0 to $\frac{\pi}{4}$) **then**
Location of the device (x_i, y_i) belongs to 1^{st} octant and device can convey from H_r with target position (x_i, v).
elseif (α is in between $\frac{\pi}{4}$ to $\frac{\pi}{2}$) **then**
location of the device(x_i, y_i) belongs to 2^{nd} octant and the device can convey from V_u with target position (u, y_i).
end if
end if
if(P < 0 && Q > 0) **then**
$\alpha \leftarrow \pi - \theta$
if(α is in between $\frac{\pi}{2}$ to $\frac{3\pi}{4}$) **then**
Location(x_i, y_i) belongs to 3^{rd} octant and the device can convey from V_u with target position (u, y_i).
elseif(α is in between $\frac{3\pi}{4}$ to π) **then**
Location of the device(x_i, y_i) belongs to 4^{th} octant and device can convey from H_l with target position (x_i, v).
end if
end if
if(P < 0 && Q < 0) **then**
$\alpha \leftarrow \pi + \theta$
if(α is in between π to $\frac{5\pi}{4}$) **then**
Location of the device(x_i, y_i) belongs to 5^{th} octant and device can convey from H_l with target position (x_i, v).
elsif (α lies in between $\frac{5\pi}{4}$ to $\frac{3\pi}{2}$) **then**
Location (x_i, y_i) belongs to 6^{th} octant and conveys from V_b with target position (u, y_i).
end if
end if
if(P > 0 && Q < 0) **then**
$\alpha \leftarrow 2\pi - \theta$
if (α lies in between $\frac{3\pi}{2}$ to $\frac{7\pi}{4}$) **then**
Location(x_i, y_i) belongs to 7^{th} octant and conveys from V_b with target position (u, y_i).
elsif (α lies in between $\frac{7\pi}{4}$ to 2π) **then**
Location (x_i, y_i) belongs to 8^{th}octant and conveys from H_r with target position (x_i, v).
end if
end if

- Step-1: Cluster formation mechanism is initiated by the IoT device i with a highest node degree.
- Step-2: Among the one-hop neighbors of initiating device, find out the device say$p$, with maximum

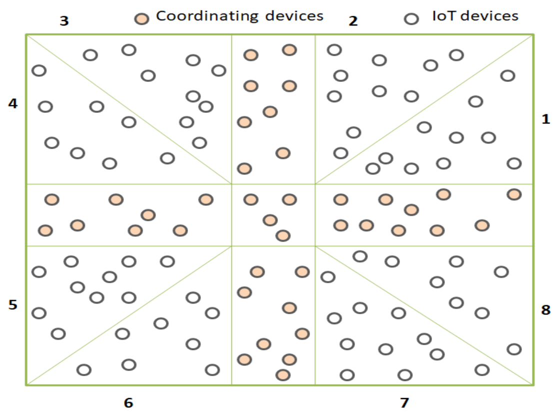

FIGURE 4. Region discovery for IoT devices.

Algorithm 3 Cluster Formation

N: Total number of devices in the network
(V_i, E_i) : Connectivity matrix of device i
▷ V_i contains the device i and its one hop neighbors.
▷ E_i contains the bi directional edge between the device in V_i
i: Initiated device
$S(i)$: Set of neighbors of device i
$L(i)$: $L(i)$ contains one hop neighbor devices of device i
$C(i)$: Set of elements in the cluster which is initially empty.
N_$C(i)$: Set of devices that are not in clusters.
i= max_{arg_j} degree(N_j) ▷ j is any arbitrary device
$S(i) = \{j, (i,j) \in E_i\}$, $C_i = \{i\}$
While($L(i) \neq \phi$)
  Find p $\in L(i)$ with maximum $| l(i) \bigcap l(p) |$
  $C(i) \leftarrow [C_i \bigcup \{p\} \bigcup \{j, \{j,p\} \in E_i]$
  N_$C_i \leftarrow [V_i \notin C_i]$
Endwhile
i= $\max_{arg_i}$ degree(N_C_i)
CH $\leftarrow$ i
Repeat step 2 for node i

common adjacency. If there is more than one device consider one with lowest ID.

- Step-3: Devices that are common in one hop neighbors of device i and p are coming under one cluster including i and p. Device i will be considered as cluster head (CH)
- Step-4: Remaining one hop neighbor of device i (Initiated device) with maximum degree start the same process for cluster formation and declare it as cluster head. The detailed process of cluster formation is illustrated in Algorithm 3.

Figure 5 shows the cluster formation of coordinating devices. According to Algorithm 3 device i is the starting device with the maximum degree and device iv is the device (p) having maximum common adjacency with the starting device i. So devices (i, ii, iii, iv and v) comes under one cluster and device i becomes cluster head, while device iv repeats the same procedure to form the cluster and become next cluster head as shown in Figure 6.

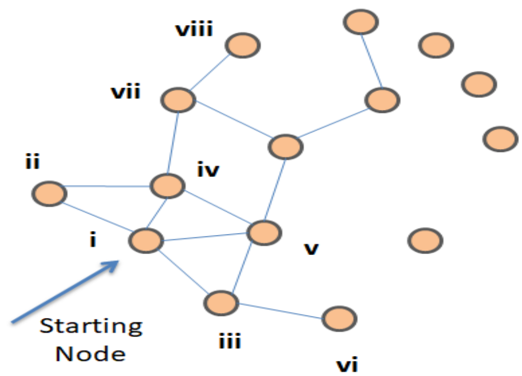

FIGURE 5. Cluster formation technique.

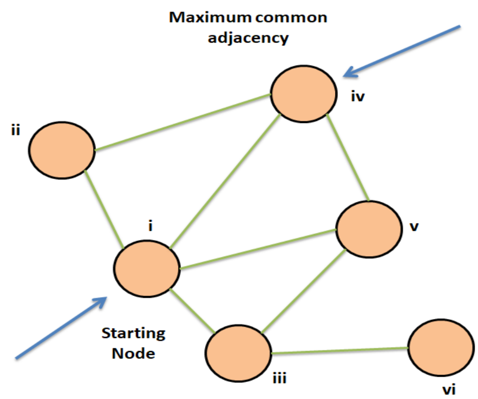

FIGURE 6. Cluster formation technique.

F. CLUSTER HEAD REELECTION

In this proposed protocol cluster head reelection occur along with new cluster formation. Following steps are followed:

- Step 1: When any cluster head device (IoT device which is selected as a cluster head) say i starts getting depleted its energy, then the cluster member device q which is having maximum common adjacency inside the cluster starts the cluster formation mechanism as described in Algorithm 3.
- Step 2: Device q will declare as the new cluster head.

G. MOBILE IoT-HUB MANAGEMENT

In this phase mobile IoT-Hub informs it's location to the cluster head devices via gateway devices. Hence all the cluster heads inside the rendezvous region have the information about the IoT-Hub's location.

When the IoT-Hub moves, it broadcasts the Beacon packet to its neighbors. IoT-Hub then chooses one of its neighboring devices to relay its position information to one of the closest cluster head inside the rendezvous region. IoT-Hub sends the location information with the help of sensor device region discovery mechanism as shown in Algorithm 4 with the help of Location Factor (LF).

Let device i wants to choose one of its neighbor from $Nb(i)$ to relay the data/ control packet. So node i will use the location factor (LF) as discussed below.

Let $k \in Nb(i)$ with coordinates(x_k,y_k), having residual energy Er_k and let Euclidean distance of device k from destination is D_k.

$$Er_{max} = \max_{k \in Nb(i)} (E_r) \tag{3}$$

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

$$LF(k) = Er_k * \frac{1}{D_k} = \frac{Er_k}{D_k} \tag{4}$$

where,

$$Er_k = \frac{Er_k}{Er_{max}}, \tag{5}$$

$$D_k = \sqrt{(x_{dest} - x_k)^2 + (y_{dest} - y_k)^2} \tag{6}$$

and

$$next\_device_i = max(LF(i)) \tag{7}$$

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

Once the IoT-Hub location information is reached to the coordinating device, it sends to its cluster head and then that cluster head send it to it's neighboring cluster heads and in the same way, now all the cluster heads have the information about IoT-Hub's new location. Figure 7 shows the mobility management of the IoT-Hub.

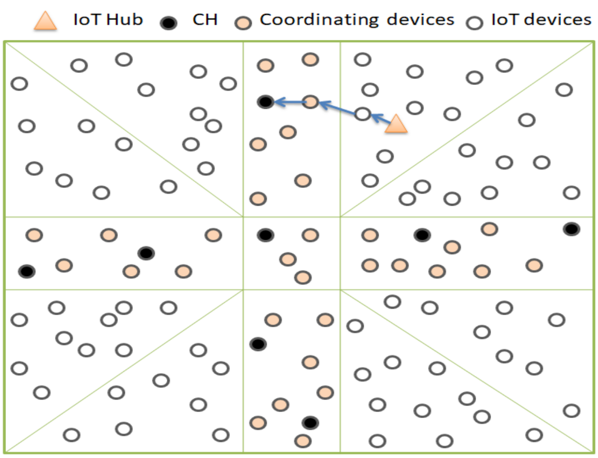

FIGURE 7. Mobile IoT-Hub management.

Algorithm 4 Mobile IoT-Hub Management

Loc_hub_x: Location information of IoT-Hub is stored in any device x.
B_x : is true if any device x labeled as the Co-ordinating device(backbone node), initialized as false.
sink_ref : IoT-Hubs reference position.
Beacon: < Beacon, id_hub >
l_rf (BeaconReply, id_x , Er_x , id_{hub});
▷ BeaconReply packet is Unicasted to the IoT-Hub. .
To send the location, IoT device uses Co-ordinating device as described in Algorithm 2. The IoT-Hub sends the Location information Packet to the device z using the LF.
l_rf (Location, id_{hub} , hub_ref , $next\_device_z$);
▷ location packet is unicasted to selected device z.
Device y or IoT-Hub send following packet to device x.
Location : < Location, id_y , hub_ref , $next\_device_y$ >
if($id_x == next\_device_y$) **then**
  if(Loc_$hub_x \neq hub_ref$) **then**
  Loc_$hub_x \leftarrow hub_ref$
    if(B_x==true) **then**
    x then send the IoT-Hub information to its CH.
    elsechoose some other device z closest to destination.
    endif
  else
  Discard the packet;
  end if
else
Discard the packet;
end if

H. IoT-Hub LOCATION RECOVERY

IoT-Hub's location information reaches to the regular IoT devices with the help of cluster heads. When the regular devices want to transmit data, it should be aware of the new IoT-Hub's position, which it gets from the cluster head inside the rendezvous region. The IoT device which wants to send the data will send Loc_{req} packet by selecting neighboring devices using Location Factor (explained in Section 4).

Once the Loc_{req} reaches to the coordinating IoT device, then this device forwards it to its cluster head. Cluster head already has the new position information of IoT-Hub, so cluster head forwards the IoT-Hub location information to the regular IoT device in the same reverse path as shown in Figure 8.

I. DATA TRANSMISSION

After getting the information about the IoT-Hub, the IoT device forward the data to the IoT-Hub with the help of neighboring devices using the location factor as shown in Section 4. IoT devices select the neighboring device depending on the residual energy and minimum distance from

Algorithm 5 IoT-Hub Location Recovery

CH:Cluster head device having IoT-Hub's location
CH_{id}:Id of the cluster head
B_x: It is true if any device is a coordinating device.
Hub_Loc: IoT-Hub's location
next_$device_x$: Any next device choose by any device x to forward the packet.
$reverse_x$: Cluster head x selects the device to send IoT-Hub's location to the requested IoT device.

Loc_{req} packet receive by device x from device y $\in$ **Nb**(x).
Loc_{req}: <Loc_{req},id_y,next_$device_y$>
if (id_x == next_$device_y$) **then**
$reverse_x \leftarrow id_y$;
if (B_x == true)
B_x forwards the Loc_{req} to its CH.
$l_r(Loc_{Reply}, CH_{id}, hub\_Loc\ reverse_x)$;
▷ Reply to the device requested .
else
▷ The device x selects the next_$device_x$ using the Location factor.
$l_r(Loc_{Req}, id_x$, next_$device_x$);
endif
else
Discard the packet
endif

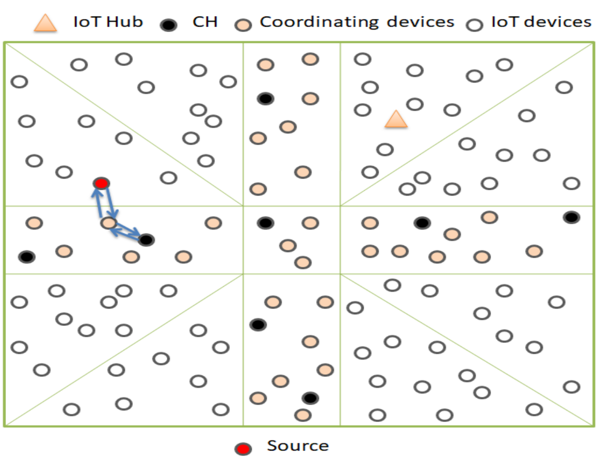

FIGURE 8. IoT-Hub location recovery.

the IoT-Hub with the help of Location Factor. On receiving the data the intermediate device forwards it to its neighbor using the same technique. The same procedure is repeated till the data reaches to the IoT-Hub as shown in Figure 9.

IV. ENERGY CONSUMPTION MODEL

In order to calculate the energy consumption of IoT device, we need to consider the transmitting and receiving energy for the devices.

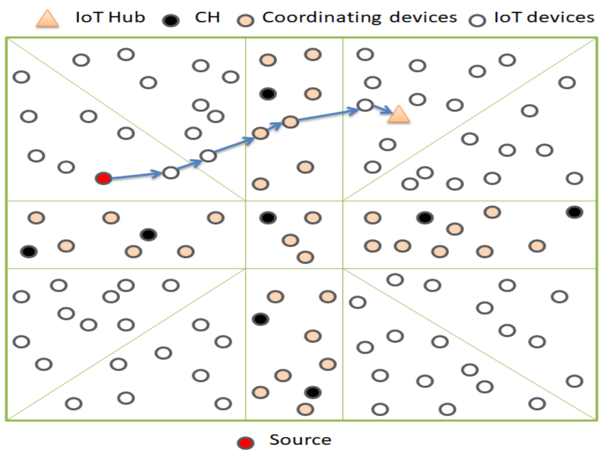

FIGURE 9. Data transmission.

Therefore, for transmitting, the energy consumption will be:

$$ET_n = E_{elec} * K * D_{min} \tag{8}$$

here E_{elec} = energy consumption in the circuit.
D_{min} = minimum distance i.e Euclidean distance
K = length of packet.
ET_n = Energy required for transmission for a IoT device.
For receiving:

$$ER_n = E_{elec} * K \tag{9}$$

Here ER_n = Energy required for receiving.
The energy consumption for Cluster head.
For transmitting:

$$ET_c = (E_{elec} + E_{fs} * d^2) * k. \tag{10}$$

or

$$ET_c = (E_{elec} + E_{mpf} * d^4) * k. \tag{11}$$

Here ET_c is the energy required for transmitting by Cluster Head device.

E_{fs} is the energy required in the free space model and E_{mpf} is the energy required in the multi-path fading model.

For receiving:

$$ER_c = E_{elec} * K. \tag{12}$$

Here ER_c is the energy required for receiving information on Cluster Head device.

V. SIMULATION AND RESULTS

On the basis of different parameters like average energy consumption, the end to end latency, packet delivery ratio and network lifetime the proposed routing protocol is compared with the existing protocols like rendezvous based routing protocol [8] and LBDD protocol [5]. A set of simulation scenario has been taken to compare the proposed model.

Finally, with the help of the simulation results, we plotted the graph to show the proper analysis. The performance of the protocol is compared for IoT Sensing Infrastructure network. Castalia simulator is used to simulate the proposed and existing protocol.

It is a test system for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and for the systems of low-control installed gadgets. To simulate the proposed model and existing models, we used following parameters illustrated in Table 2.

TABLE 2. Simulation parameter.

Simulation Parameters	values
Simulator used	Castalia Simulator (version 3.2)
IoT Sensing Network area	100*100 m^2
Number of IoT devices	(25, 50, 125, 100, 125, 150, 175, 200)
IoT-Hub speed	5m/sec
Mobility model	Gauss Mobility model
Simulation time	600s
MAC protocol	Tunable Mac
Initial energy of devices	20J

A. AVERAGE ENERGY CONSUMPTION

In the proposed work, energy consumed by IoT devices is less than the existing rendezvous based and LBDD routing protocol. There are many factors that affect the energy consumption of proposed model such as single hop communication between cluster heads, load balancing, and less control packet transmission.

From Figure 10, we can see that LBDD consumes the highest energy due to more control packet overhead. It stores the data from the source device and floods IoT-Hub query in the rendezvous region. In Rendezvous-based protocol some of the backbone devices participate in the tree structure construction which increases the energy consumption due to increased control packet overhead. Due to less control packet overhead, the proposed protocol gives more efficient results than the existing protocols.

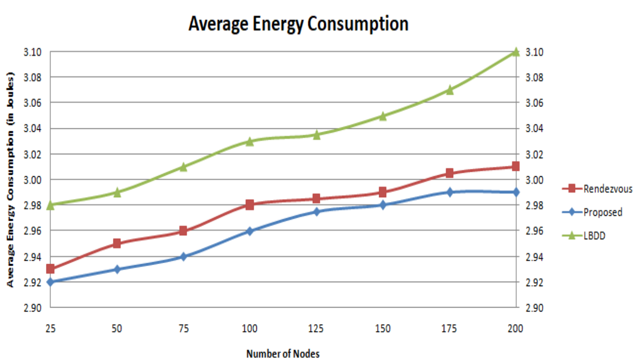

FIGURE 10. Average Energy Consumption.

B. END TO END DELAY

The End to End delay or one-way delay (OWD) refers to the time taken to find the IoT-Hubs location and transfer the data to IoT-Hub. Figure 11 shows that the End to End delay of the proposed routing protocol is less than the other two existing protocols. There are many reasons for this, first is the management of IoT-Hub mobility. Secondly, source device gets quick knowledge about IoT-Hub's location. When the IoT-Hub changes its position it immediately sends the location information to the cluster heads. Lastly, there is a limited number of coordinating devices are involved in getting IoT-Hub's location.

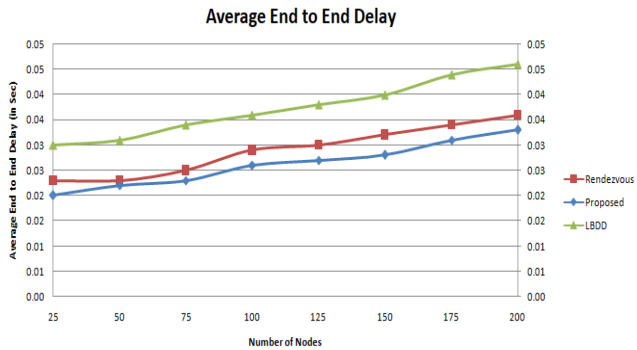

FIGURE 11. End to end delay.

In LBDD, inline nodes transmit the data, when they know the IoT-Hubs location. Rendezvous-based also transmit data instantly to backbone tree. The tree will forward data to IoT-Hub as it knows the location of the IoT-Hub which increases the delay. The proposed method takes less time than the other two protocols.

C. PACKET DELIVERY RATIO

Packet delivery ratio can be defined as the ratio of the number of data packets that reach the IoT-Hub to the total number of packets sent. The packet delivery ratio in the routing protocol is more than the existing protocol as shown in Figure 12. The Possibility of packet loss is less in the proposed work.

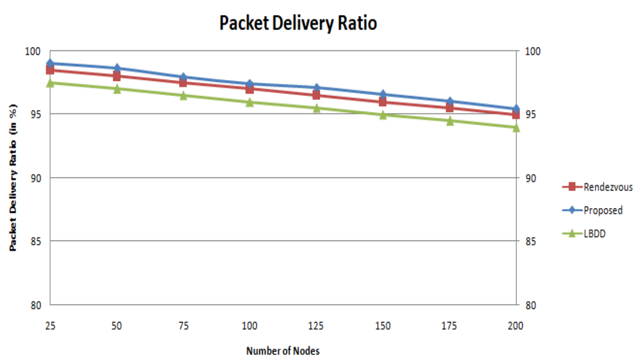

FIGURE 12. Packet delivery ratio.

In LBDD, the data stored at inline nodes are transmitted immediately when they know the IoT-Hubs location. In Rendezvous-based as the tree is always in connection with the sink, therefore the delivery ratio is high. In the proposed protocol coordinating devices get the position immediately if IoT-Hub is relocated. Therefore, Packet delivery ratio is higher than the existing protocols.

D. NETWORK LIFETIME

Lifetime of the IoT Sensing network is the time elapsed till the first device of the network dies. In the proposed work the lifetime of the IoT sensing network is more than the existing model shown in Figure 13.

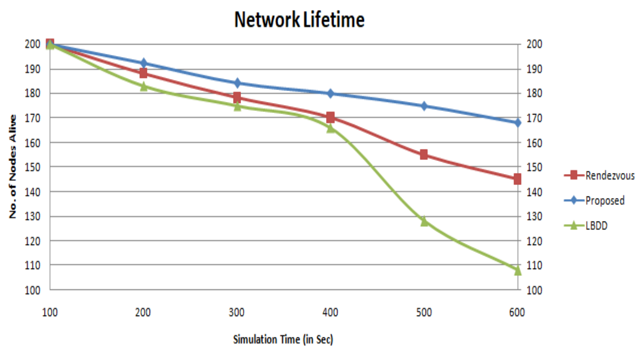

FIGURE 13. **Network lifetime.**

Comparing with other protocols, the network lifetime of the proposed protocol is more due to the reason that it consumes few control packets and it finds an optimal path for transmitting the data as compared to LBDD and rendezvous routing protocol.

VI. CONCLUSION

This paper proposed rendezvous routing protocol in Cluster based mode for IoT Sensing network to build scalable cyber-physical-social networking infrastructure. In the proposed model there are many phases such as: neighbor device detection, device region discovery, mobile IoT-Hub management, cluster selection, Cross area development, IoT-Hub location recovery and data transmission. In the proposed model, Clusters are constructed inside the rendezvous region and communication takes place among cluster heads with single hop distance. This will diminish energy depletion and increase the IoT network lifetime. We have also compared the proposed model with the existing models and found that the model is energy efficient, which increases the lifetime of the network and packet delivery ratio.

ACKNOWLEDGMENT

This paper was presented at the International Conference on Computing, Communication and Automation, May 5–6, 2017 [43].

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.
[2] 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.
[3] 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.*, to be published.
[4] 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.
[5] E. Ben Hamida and G. Chelius, "A line-based data dissemination protocol for wireless sensor networks with mobile sink," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 2201–2205.
[6] 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.
[7] 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.
[8] S. Sharma *et al.*, "Rendezvous based routing protocol for wireless sensor networks with mobile sink," *J. Supercomput.*, vol. 73, no. 3, pp. 1168–1188, Mar. 2017.
[9] Z. H. Mir and Y.-B. Ko, "A quadtree-based data dissemination protocol for wireless sensor networks with mobile sinks," in *Proc. IFIP Int. Conf. Personal Wireless Commun. (PWC)*. Berlin, Germany: Springer, Sep. 2006, p. 447.
[10] 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.
[11] S. 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.
[12] D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and big data: An architecture with data flow and security issues," in *Cloud Infrastructures, Services, IoT Systems for Smart Cities*. Cham, Switzerland: Springer, 2017, pp. 243–252.
[13] S. Olariu and I. Stojmenovic, "Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting," in *Proc. 25th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2006, pp. 1–12.
[14] J. Luo and J. P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," in *Proc. 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 3, Mar. 2005, pp. 1735–1746.
[15] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. Mohanty, and A. Y. Zomaya, "Secure and sustainable load balancing of edge data centers in fog computing," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 60–65, May 2018.
[16] 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.
[17] S. Jain, S. Sharma, and N. Bagga, "A vertical and horizontal segregation based data dissemination protocol," in *Emerging Research in Computing, Information, Communication and Applications*. New Delhi, India: Springer, 2016, pp. 401–412.
[18] D. Puthal, "Lattice-modelled information flow control of big sensing data streams for smart health application," *IEEE Internet Things J.*, to be published.
[19] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc. 5th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw. (ICMCN)*, Aug. 1999, pp. 263–270.
[20] C. Cimen, E. Cayirci, and V. Coskun, "Querying sensor fields by using quadtree based dynamic clusters and task sets," in *Proc. Mil. Commun. Conf. (MILCOM)*, vol. 1, Oct. 2003, pp. 561–566.
[21] A. Salim, W. Osamy, and M. Ahmed Khedr, "IBLEACH: Intra-balanced LEACH protocol for wireless sensor networks," *Wireless Netw.*, vol. 20, no. 6, pp. 1515–1525, Aug. 2014.
[22] C.-T. Lin *et al.*, "IoT-based wireless polysomnography intelligent system for sleep monitoring," *IEEE Access*, vol. 6, pp. 405–414, 2018.
[23] 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.
[24] J. Rivera and R. van der Meulen, "Gartner says the Internet of Things installed base will grow to 26 billion units by 2020," Stamford, CT, USA, Tech. Rep., Dec. 2013. [Online]. Available: https://www.gartner.com/newsroom/id/2636073
[25] D. Fletcher, "Internet of Things," in *Evolution of Cyber Technologies and Operations to 2035*. Springer, 2015, pp. 19–32.

[26] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May 2016.

[27] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[28] H. Bauer, M. Patel, and J. Veira, "The Internet of Things: Sizing up the opportunity," McKinsey, New York, NY, USA, Tech. Rep., Dec. 2014. [Online]. Available: https://www.mckinsey.com/industries/semiconductors/our-insights/the-internet-of-things-sizing-up-the-opportunity

[29] D. Puthal, "Secure data collection and critical data transmission technique in mobile sink wireless sensor networks," M.S. thesis, Dept. Comput. Sci., Nat. Inst. Technol., Rourkela, Rourkela, Odisha, 2012.

[30] 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.

[31] C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, "Big-sensing-data curation for the cloud is coming: A promise of scalable cloud-data-center mitigation for next-generation IoT and wireless sensor networks," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 48–56, Oct. 2017.

[32] M. Elshrkawey, S. M. Elsherif, and M. E. Wahed, "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. 2017.

[33] 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, 2017.

[34] 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.

[35] H. El-Sayed *et al.*, "Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment," *IEEE Access*, vol. 6, pp. 1706–1717, 2018.

[36] 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.

[37] G. Xing, M. Li, T. Wang, W. Jia, and J. Huang, "Efficient rendezvous algorithms for mobility-enabled wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 1, pp. 47–60, Jan. 2012.

[38] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," *Comput. Netw.*, vol. 56, no. 7, pp. 1951–1967, 2012.

[39] 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.

[40] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A secure big data stream analytics framework for disaster management on the cloud," in *Proc. 18th IEEE Int. Conf. High Perform. Comput. Commun.*, 2016, pp. 1218–1225.

[41] 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.

[42] D. Puthal, X. Wu, S. Nepal, R. Ranjan, and J. Chen, "SEEN: A selective encryption method to ensure confidentiality for big sensing data streams," *IEEE Trans. Big Data*, to be published.

[43] R. K. Lenka, A. Rath, A. Aggarwal, and S. Sharma, "Cluster-based rendezvous routing protocol for wireless sensor network," in *Proc. Int. Conf. Comput., Commun. Autom.*, Dec. 2017, pp. 748–752.

[44] J. Zhu, J. Liu, Z. Hai, and Y.-G. Bi, "Research on routing protocol facing to signal conflicting in link quality guaranteed WSN," *Wireless Netw.*, vol. 22, no. 5, pp. 1739–1750, Jul. 2016.

[45] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyberthreats," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 24–27, Oct. 2017.

RAKESH KUMAR LENKA received the M.Tech. degree from the Motilal Nehru National Institute of Technology, Allahabad, India. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Veer Surendra Sai University of Technology, Burla, India. He is also an Assistant Professor with the Department of Computer Science and Engineering, International Institute of Information Technology at Bhubaneswar, Bhubaneswar. His research interests include compiler design, Internet of Things, wireless sensor networks, and big data analysis.

AMIYA KUMAR RATH received the B.E. degree in computer from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, 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 systems. He is currently a Professor with the Department of Computer Science and Engineering, Veer Surendra Sai University of Technology, Burla, India. He has contributed over 80 research level papers 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 network, power minimization, evolutionary computation, and data mining. He was elected as an Accessor of the National Assessment and Accreditation Council, India.

ZHIYUAN TAN received the Ph.D. degree from the University of Technology Sydney, Australia. He was a Post-Doctoral Researcher with the Services, Cybersecurity and Safety Research Group, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, The Netherlands. He is currently a Lecturer with the School of Computing, Edinburgh Napier University, U.K. His research interests are computer and network security, pattern recognition, and machine learning.

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

DEEPAK PUTHAL received the Ph.D. degree in computer science from the University of Technology Sydney (UTS), Australia. He is currently a Lecturer (Assistant Professor) with the Faculty of Engineering and IT, UTS. His research interests include cyber security, Internet of Things, distributed computing, and big data analytics. He has authored over 50 peer-reviewed research articles. He was a recipient of the 2017 IEEE Distinguished Doctoral Dissertation Award by the IEEE Computer Society and STC on Smart Computing. He is serving as an Associate Editor for the IEEE TRANSACTIONS ON BIG DATA, *IEEE Consumer Electronics Magazine*, the *International Journal of Communication Systems* (John Wiley & Sons), and *Internet Technology Letters* (John Wiley & Sons).

N. V. R. SIMHA received the B.Tech. degree from Kakatiya University in 2016. He is currently pursuing the M.Tech. degree from the International Institute of Information Technology at Bhubaneswar, Bhubaneswar. His research interests include wireless communication, networking, and routing in wireless sensor networks.

MUKESH PRASAD received the master's degree in computer application from Jawaharlal Nehru University, New Delhi, India, in 2009, and the Ph.D. degree from the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan. He is currently a Lecturer (Assistant Professor) with the School of Software, University of Technology Sydney, Australia. His current research interests include machine learning, big data, pattern recognition, fuzzy systems, and neural networks. He has published several journal and international conference papers.

ROHIT RAJA received the Ph.D. degree in computer science and engineering form Dr. C. V. Raman University in 2016. He is currently a Professor with the CSE Department, Sreyas Institute of Engineering and Technology, Hyderabad, India. He has authored several journal and conference papers. His main research interests include face recognition and identification, digital image processing, signal processing, and wireless networks.

SHANKAR SHARAN TRIPATHI received the M.Tech. degree from the Shri Shankaracharya College of Engineering and Technology, Bhilai, India, in 2013. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Shri Shankaracharya College of Engineering and Technology. His research interests include wireless networks and Internet of Things.