

Article

Cluster-Based Routing Protocol with Static Hub (CRPSH) for WSN-Assisted IoT Networks

Rakesh Kumar Lenka ¹, Manjur Kolhar ², Hitesh Mohapatra ^{3,*}, Fadi Al-Turjman ⁴ and Chadi Altrjman ⁵

- ¹ Department of Computer Science and Engineering, International Institute of Information Technology, Bhubaneswar 751003, OD, India; rakeshkumar@iiit-bh.ac.in
- ² Department of Computer Science, College of Arts and Science, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia; m.kolhar@psau.edu.sa
- ³ Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522302, AP, India
- ⁴ Artificial Intelligence Engineering Department, Research Center for AI and IoT, AI & Robotics Institute, Near East University, North Cyprus via Mersin 10, Nicosia 99138, Turkey; fadi.alturjman@neu.edu.tr
- ⁵ Department of Chemical Engineering, Waterloo University, Waterloo, ON N2L 3G1, Canada; cmfaltrj@uwaterloo.ca
- * Correspondence: hiteshmahapatra@gmail.com

Abstract: The Internet of Things (IoT) is an evolving concept that has achieved prominence in the modern era. An autonomous sensor-equipped device is the major component of WSN-assisted IoT infrastructure. These devices intelligently sense the environment, automatically collect the data, and deliver the information to paired devices. However, in WSN-assisted IoT networks, energy depletion and hardware faults might result in device failures. Additionally, this might affect data transmission. A reliable route significantly reduces data retransmissions, which can help in congestion reduction and energy conservation. Generally, the sensor devices are typically deployed densely throughout the WSN-assisted IoT networks. A high number of sensor devices covering a monitoring area might result in duplicate data. The clustering method can be used to overcome this problem. The clustering technique reduces network traffic, whereas the multipath technique ensures path reliability. In CRPSH, we used the clustering technique to reduce the duplicate data. Moreover, the multipath approach can increase the reliability of the proposed protocol. CRPSH is intended to minimize the overhead associated with control packets and extend the network's lifetime. The complete set of simulations is carried out using the Castalia simulator. The proposed protocol is found to reduce energy consumption and increase the lifetime of IoT infrastructure networks.

Keywords: Internet of Things; wireless sensor network; routing; green IoT



Citation: Lenka, R.K.; Kolhar, M.; Mohapatra, H.; Al-Turjman, F.; Altrjman C. Cluster-Based Routing Protocol with Static Hub (CRPSH) for WSN-Assisted IoT Networks. *Sustainability* **2022**, *14*, 7304. <https://doi.org/10.3390/su14127304>

Academic Editor: Samad Sepasgozar

Received: 3 May 2022

Accepted: 6 June 2022

Published: 15 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In a multihop scenario, the sensor device transfers the data to the IoT hub via intermediary sensor devices. WSN-assisted IoT networks are energy constraint networks. So, energy-efficient routing methods are necessary for WSN-assisted IoT networks operating in an energy-constrained environment. However, in WSN-assisted IoT networks, energy depletion and hardware faults might result in device failures. Additionally, this might affect data transmission. A reliable route significantly reduces data retransmissions, which can help in congestion reduction and energy conservation. Generally, the sensor devices are typically deployed densely throughout the WSN-assisted IoT networks. A high number of sensor devices covering a monitoring area might result in duplicate data. The clustering method can be used to overcome this problem. The Cluster Heads (CH) collect data from Cluster Members (CM) prior to sending them to the hub. The clustering technique reduces network traffic, whereas the path reliability is ensured by the multipath technique. These two approaches encourage the development of a hybrid technique that incorporates the benefits of both strategies [1,2].

Devices in WSN-assisted IoT networks must hunt for a way up to the IoT hub for data transmission [3]. Although the device's technical capabilities are improving all the time, the device's battery capacity is not keeping up [4]. IoT gadgets use nonrechargeable limited-power batteries. It is also challenging to replace their battery while the devices are in use. Moreover, we need advanced power-saving schemes to make these IoT technologies more adaptable. Due to the energy constraints and limited memory capacity of these IoT devices, we require more energy-efficient routing protocols to route data to the IoT hub [5,6].

A WSN-assisted IoT network is a unit of Low-power and Lossy Networks (LLNs) which are categorized as minimal power and energy-constrained devices that are interrelated with links, where LLN devices can act as data originator and router [7]. In LLNs, power conservancy and network lifetime improvement are the foremost challenges [8]. The routing over LLNs' WG of the Internet Engineering Task Force (IETF) produced specifications for both the RPL protocol (RFC 6550) and a set of related extensions for various routing metrics, objective functions, and multicasts. The wireless links in LLN are lossy because of the quality of radios and minuscule size of LLN, and the routing protocols in LLN provide routing within the network. The state-of-the-art routing protocols for WSN-assisted IoT networks can be classified into three types as flat, hierarchical, and location-based protocols [9].

All sensor devices in *flat-type routing* protocols perform an equal role in acquiring information from the environment and relaying it to the IoT hub. The distance between the devices is computed based on the received signal strength in *location-based routing* protocols. This information is used for efficient data transfer. *Hierarchical routing protocols* are the most widely used routing protocols for WSN-assisted IoT networks. They partition the whole network area into different regions. Each partition has a master node and many member nodes. The master node is responsible for gathering data from the member nodes and transmitting it to the hub. Additionally, it is capable of effectively balancing the load on the sensor devices by assigning distinct tasks to distinct devices. Hierarchical routing is a viable option for lowering energy consumption by eliminating redundant data transmission. Due to its high energy efficiency, it outperforms other types of routing protocols [10–14].

Section 2 presents an extensive literature survey and Section 3 describes the system model. Section 4 focuses on the protocol's description as well as the algorithms that are used to develop it. Section 5 presents the findings of the simulation and Section 6 provides a conclusion and future research direction.

2. Literature Review

Various routing methods for WSN-aided IoT Networks have been suggested in recent years [15–20]. In this part, we look at a few of the many types of new protocols. The LBDD routing protocol defines a large vertical strip of devices centered horizontally on the deployment area [21]. It is separated into g -sized sets once more. In-line devices are those that are connected to this virtual infrastructure. The data from the device is sent down the line and stored by the first in-line device that comes across it. When an IoT device detects any data, it sends it to the closest in-line device. When a hub requests data, it sends a vertical request to the virtual route [22]. First, the aligned device delivers it in both directions along the line's course. When a query is sent to the relevant data-containing sensor devices, the devices submit the data immediately to the IoT hub. The amount of queries issued might sometimes outnumber the data. Broadcasts are used by LBDD to transmit data requests over the network [23]. The line structure may be quickly and cheaply created. This line must be sufficiently wide to prevent hotspots. It lowers energy usage while increasing overhead. The AN Position Information Request packet (ANPIREQ) is sent from the source device to the ring. When the ring devices receive the request, they transmit the AN Location Information Response (ANPIRES) packet to the source, which provides the current AN's position information. The source can transmit data to the AN after receiving the response packet from the ring node. By including a small number of

nodes in the ring, the Ring Routing protocol minimizes control packets. The anchor device's location is requested by the source device [24]. The anchor device location information packet is sent by the ring devices in response. The data is transmitted to the anchor device once the source device has the anchor device's position information. By aggregating the smallest number of sensor devices into the closed loop, the impacts of control packets are decreased. The RRP1 protocol is designed to operate with small, inefficient broadcasts [25].

The Railroad protocol takes advantage of the rail infrastructure to store all of the metadata associated with event data. In railroad routing, there are four main procedures. Rail construction, event notification, query request, and data transmission are among these processes [26]. When the gadget detects data, it sends the metadata associated with it to the closest station (group of rail devices). Platform devices are the equipment in the station. The process of rail building occurs just once during the set-up phase. To see if a device is on the rail, it has to know how far away it is from the nearest border device and network center. The rail is notified of the event summary via event notification messages. When the rail device receives the message, it creates a new station and sends the message to the station's platform devices. The railroad differs from LBDD in that it introduces a significant feature: the hub's inquiries are unicast rather than broadcast. The stations should be wide enough to accommodate the rail width. Finally, because the inquiry must travel a greater distance, the railroad protocol delays data transmission more than the LBDD protocol. To obtain the information, the hub sends out a query. In three stages, this question is transmitted to the source. Query forwarding on the rail, query circulation around the rail, and query notification to the source are all included. The inquiry is sent from the hub to its neighboring device and subsequently to devices along the way to the train. The inquiry circulates with the help of direction information after it enters the train. In the middle of its journey, it also inspects all of the stations. If any station has relevant data that the hub requires, the platform device sends a query notification message to the source. After receiving the query notification message, the source sends the data to the hub.

The whole network region is partitioned into four equal planes by one horizontal and one vertical strip in the Rendezvous-Based Routing Protocol (RBRP). The rendezvous region is a horizontal and vertical strip of land. This virtual structure divides the network into four sections: 1—horizontal left, 2—horizontal right, 3—vertical up, and 4—vertical down. This intersection acts as a gathering spot. Devices that operate in this cross section are known as backbone devices. A tree was created in this area and some of the backbone devices are part of it. This tree is responsible for data transmission from the source to the hub and from the hub to the source [27]. The hub position is known by the devices that participate in tree creation, while the hub position is unknown to the other backbone devices. Space partitioning is accomplished using the quadtree structure of the network via the quadtree-based routing protocol (QDD). The following assumptions guide the development of this protocol: All stimuli and hubs are movable, but IoT devices are stationary and aware of their location. They are also familiar with their one-hop neighbors. The IoT devices are aware of the whole WSN-assisted IoT network, which is defined as $2m \times 2m$, where $m = \log_2(N)$. For data and packet delivery, this protocol uses a greedy forwarding mechanism [28].

The building quadtree structure in QDD is modest as compared with other hierarchical techniques. The QDD has been unable to resolve the hotspot issue. For WSN-assisted IoT networks, the Centroid-Based Routing Protocol (CBRP) suggested an energy-efficient data routing protocol. It establishes the Candidate Cluster Head (CH) device, which ensures a consistent allocation of energy in the cluster. Cluster formation is delegated to the BS, which helps to reduce cluster formation overhead. The data packets are sent using a threshold distance. Data loss happens when the distance exceeds the threshold [29]. The procedure for re-electing cluster heads has yet to be established. The WSN-assisted IoT network is divided into sectors via the SCBC (Sector-Chain-Based Clustering Routing Protocol) (cluster). For each cluster, it creates a chain, with the chain leader functioning as the cluster head (CH) and secondary cluster head (SCH), both of which contain considerable residual energy. The SCH

has the smallest distance between candidate nodes and the network's base station (BS). The network's energy dissipation is decreased by using chains for data transfer. When compared with the CH, the SCH is used to save energy. The Base Station (BS) establishes clusters and selects a cluster leader, resulting in higher energy use in following rounds [30].

The LEACH protocol is available in a variety of variants that improve its performance. Heinzelman et al. propose LEACH-C, which uses a fixed number of CHs in subsequent rounds and assigns CHs to clusters via a base station [31]. Clusters are formed only once during the setup phase of LEACH-F and persist for the duration of the network [32]. New IoT devices are not permitted to join the network in this configuration. The network is controlled by BS, which transmits data via single-hop communication. Biradar et al. [33] propose a multihop LEACH, in which an optimal multihop tree is constructed between all CHs, with the IoT hub as the root. This path is responsible for communication in the network. Another version, MS-LEACH, uses one-hop and multihop communication for transmission, which depends on the cluster size proposed by Qiang et al. [34]. Farooq et al. propose an MR-LEACH that divides the entire network area into layers depending on the hop distances among the cluster heads [35]. The data is transmitted from the lower layer's CH to the nearest upper layer's CH until it reaches the IoT hub. The existing protocols [32–35] increase the network lifetime but have a problem with hotspots in the network because of overtraffic near the base station. Researchers have tried to solve this problem by delivering more energy-efficient routing protocols such as a mobile IoT hub, multihop communication, constrained mobility of the IoT hubs, and grid-based routing protocols.

Sanchez et al. [36] propose the GMR multicast routing protocol. It mainly deals with multicast messages produced by the source IoT device. It finds the subset of IoT devices to send messages to all destinations with less bandwidth and utilizes minimal sensor resources such as battery, memory, and CPU usage. Here, the IoT devices know their position, and periodic beacons are used to send their position information to their neighboring IoT devices. The IoT devices are selected by using their position and running GMR for sending the data to destinations. The best subset of IoT devices can reduce the distance to destinations and reduce the overheads. If some neighbors fail to reduce the distance to the destination, then face routing is used to exit local minima until it finds a new IoT device.

Buttayan and Schaffer proposed the PANEL routing protocol [37], which divides the network area into clusters geographically and deploys the IoT devices randomly. A PANEL elects the aggregator IoT devices in each cluster. Each aggregator IoT device receives queries from the IoT hub. Here, the processing time is divided into epochs, and for each epoch, a different aggregator IoT device is selected for load balancing in the network. PANEL routing may be of two types. Routing within the cluster is called intracluster routing. Here, the message from IoT devices is routed to current or former aggregator IoT devices. Routing among the clusters is called intercluster routing, where the messages come from a distant source. It suffers from IoT device depletion when cluster connections become divided, which causes the election of more than one within-cluster aggregator. Akl and Sawant proposed a Grid-based Coordinated Routing protocol in which the total network area is divided into small-sized (user-specified) grids [38]. Each grid has a coordinating IoT device that determines the routing. The source IoT device floods data and queries to the network. The IoT hub responds to these queries by sending information back on the reverse path. This process continues until any coordinating IoT device's energy becomes depleted or the connectivity is lost between the IoT hub and the source due to the network's partition. A new coordinating IoT device is selected from the grid based on its ID. For example, the second-largest ID is selected when the first becomes exhausted. To preserve energy, noncoordinating IoT devices can sleep by shutting their radio signal.

Das et al. proposed a hierarchical Rendezvous Point Multicast (HRPM) protocol that divides a group into smaller groups [39]. A distributed geographic hashing concept is used for building and maintaining a hierarchy with no additional cost. The network field is divided into square cells of equal size until we reach a cell with a manageable number of IoT devices, and each cell is controlled by an Access Point (AP). Two approaches are used to increase the scalability of location-based multicast: distributed mobile geographic hashing and the hierarchical breakdown of large multicast groups. They provide lightweight hierarchical membership management, reducing per-packet encoding overhead without the significant expense of maintaining distributed state at mobile nodes. The members of the multicast tree fix the rendezvous point as a group manager. A virtual source to AP tree is built from the source that transmits data to this (source to AP) tree. An overlay tree consisting of AP members transfers packets to IoT devices in the group, and Face routing handles the holes in HRPM.

Koutsonikolas et al. proposed a Hierarchical Geographic Multicast Routing Protocol (HGMR) that uses both GMR and HRPM for static networks, providing forward efficiency and reduced encoding overhead [40]. In HGMR, the subgroups' hierarchy is designed to reduce encoding overhead. HRPM's unicast method is used for delivering the data from the source to the AP tree, and GMR's broadcast-based forwarding method is used for AP to member tree to reduce transmission numbers. AP monitors destination IoT devices in every cell, and these are selected by using the localized neighbor selection method of the GMR. The trees in HGMR are not overlay as in HRPM. Banimelhem and Khasawneh propose a grid-based multipath routing protocol (GMCAR) that avoids congestion and supports QoS traffic for WSN [41]. This protocol is proactive, hierarchical, and supports multipath. The protocol consists of three phases: grid formation, building routing tables, and data transmission phases. The entire network is divided into small, square-shaped grids of predefined size, containing a master and nonmaster IoT device. It is the first protocol to use the concept of finding the diagonal paths between the master IoT device and the IoT hub. It also considers the density of IoT devices as a decision factor for data forwarding. The master IoT device is responsible for data routing from nonmaster IoT devices and other master IoT devices to the IoT hub. A routing table is built for each master IoT device to know other masters' IoT device positions to send the data diagonally until it reaches the IoT hub. The IoT hub sends a flooding message to enable master IoT devices to find the paths from the grid to the IoT hub. Master IoT devices collect the data from grid members and select the next master IoT device to send the data. This process is continued until the energy of the master IoT device is exhausted. The master IoT device selects a new IoT device based on residual energy. The GMCAR uses two routing techniques for high and low traffic to boost network lifetime.

An energy-aware grid-based routing technique named EAGER for WSN is proposed by Chi and Chang [42]. Grids are constructed in the network, and each grid is assigned with a unique grid ID. An IoT device is selected as a grid head in each grid, which has information about the neighboring grid heads. The TDMA technique is used for keeping the grid heads active depending on the sum of coordinates. The grid head of the source IoT device sends a request packet for path building. The IoT hub's Local Grid Head (LGH) replies with a reply packet that reached the source's LGH, so this path transmits the data. When the IoT hub moves to another location, the IoT hub's path is extended by the IoT hub, and rerouting is used for constructing a path to the IoT hub. Khan et al. proposed VGDR, where the network area is divided into grids containing equally sized cells [43]. Cell headers are the IoT devices close to the center of the cell. For the communication between neighboring cells, gateway IoT devices are elected. Cell headers can keep the information regarding the IoT hub's present location by constructing a virtual backbone structure with gateway IoT devices. Data communication takes place between member IoT devices and their closest cell header. Cell headers collect the data from member IoT devices and transfer them to mobile IoT hubs. The IoT hub flows in the network to collect data

from the border cell header. The route's re-adjustment can be performed by a border cell header, which is very close to an IoT hub.

The network reliability is the main concern for the existing routing protocols such as PCMRP. It creates a multipath by flooding control packets across the network. This is a significant contributor to the increase in control packet overhead. Additionally, the multipath is reconstructed if any device becomes the source. This adds to the protocol's overhead [44]. The REDCL method prioritizes the selection of a fewer number of active reporting nodes (ARNs) in hotspot areas over the selection of more ARNs in nonhotspot areas. The REDCL method converges the paths of several ARNs monitoring an event outside of nonhotspot zones and sends them to the hub after data aggregation. The hotspot area's ARNs are unable to transfer data directly to the hub. They must communicate with the hub through nonhotspot ARNs. This intern places an additional burden on nonhotspot ARNs. As a result, the energy consumption of nonhotspot ARNs is rather high, therefore increasing the overall energy consumption of the network [45].

Suresh and Sharma proposed VGBST consists of a group of cells that are responsible for rebuilding new routes depending on the present location information of the IoT hub [46]. A virtual infrastructure is designed by dividing the entire field into grids of equal-sized cells. The selection of cell headers in the network depends on the IoT devices, which are very close to the cell's center, which monitors the mobile IoT hub's position. The rest of the IoT devices other than CHs send data to the closest CH, and this CH forwards to the CH adjacent to it by using gateway IoT devices. Grid-Based Reliable Routing (GBRR) was proposed by Meng et al., where communication quality helps choose the succeeding communication hop [47]. It is performed by creating virtual square grids of equal size such that each grid contains a few IoT devices. Total energy consumption is minimized with the help of the present position of IoT devices and grids, which is helpful for clustering. A cluster can occupy one or more grids, and the elected CH is responsible for managing the intracluster and intercluster communication. The routing algorithm helps to construct the productive paths inside a cluster and between the clusters to avoid overloading. All IoT devices are not used in the path while transferring the data from the source IoT device to the base station.

A Mode-Switched Grid-Based Sustainable Routing Protocol (MSGR) for Wireless Sensor Networks is an energy-efficient routing protocol which partitions the entire sensing region into virtual grids of equal size [48]. In this scheme, each grid IoT device is selected as a grid head, and the path to the IoT hub is constructed using the grid head. This scheme improves network lifetime by switching the grid heads between active and sleep modes such that every grid head does not take part in establishing a path to the IoT hub at the same time. A path is built to the IoT hub by the active grid heads. Data is sent directly to the IoT hub by active grid heads in the IoT hub path. From the grid head's coordinate, we can infer whether it is in active or sleep mode. Table 1 illustrates the comparison among the existing protocols by considering several factors.

Table 1. Comparison of Routing Protocols for WSN-assisted IoT Networks.

Protocol	Classification	Mobility	Energy	Scalability	Delay
CCS [49]	Chain Based	No	Very Low	Low	Large
EBCRP [50]	Chain Based	No	Very Low	Low	Large
PEGASIS [51]	Chain Based	No	Very Low	Very Low	Very Large
CHIRON [52]	Chain Based	No	Moderate	Low	Small
BATR [53]	Tree Based	No	Low	Low	Large
EADAT [54]	Tree Based	No	Moderate	Low	Large
PEDAP [55]	Tree Based	Yes	Moderate	Low	Moderate
ETR [56]	Tree Based	No	Moderate	Moderate	Moderate
TTDD [57]	Grid Based	Yes	Very Low	Moderate	Very Large

Table 1. Cont.

Protocol	Classification	Mobility	Energy	Scalability	Delay
PANEL [37]	Grid Based	No	Moderate	Moderate	Moderate
HGMR [40]	Grid Based	No	Low	High	Moderate
GMCARE [41]	Grid Based	No	Moderate	Moderate	Moderate
RRP1 [25]	Area Based	Yes	Moderate	Moderate	Moderate
LBDD [21]	Area Based	Yes	Moderate	Moderate	Moderate
VLDD [58]	Area Based	Yes	Moderate	Moderate	Large
RRP2 [26]	Area Based	Yes	Moderate	Moderate	Large

3. System Model

3.1. Assumptions

The WSN-assisted IoT network is made up of numerous sensor devices that are connected via a radio communication link operating within the radio range R . When the distance between two devices is less than the radio range R , the communication link is considered direct (one-hop); otherwise, the communication link is considered indirect (multihop). The network is comprised of k sensor devices and an IoT hub. The IoT hub is equipped with an infinite amount of memory, processing, and battery power. The devices can estimate the Received Signal Strength Indication (RSSI) value of the received signal. This protocol is well-suited for applications that require periodic sensing.

3.2. Energy Consumption Model

We should incorporate receiving and sending energy for IoT devices when calculating IoT device energy usage. Let $E_{Trans}(n, d)$ denote the cost of transmitting n bits of data over a distance of d meters and $E_{Recv}(n)$ denote the cost of receiving n bits of data over the same distance [59].

For transmitting n bits:

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

For receiving n bits:

$$E_{Recv}(n) = E_{Embb} * d. \quad (1)$$

The energy spent by IoT device in sleeping state is:

$$E_{sleep}(t) = E_{low} * t. \quad (2)$$

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.

Any IoT device in the network consumes a total energy of:

$$E_{Total} = E_{Trans}(n, d) + E_{Recv}(n) + E_{sleep}(t). \quad (3)$$

4. Proposed Protocol

The protocol under consideration, CRPSH, discovers all possible paths prior to their use. This technique is appropriate for static networks. CRPSH uses a clustering technique that needs the path between the CH and the hub. The hub is in charge of calculating the route discovery and regulating the energy consumption of every sensor device in the network. It is divided into four phases: peer discovery, cluster formation, data transfer, and re-clustering and rerouting.

4.1. Peer Discovery

After sensor devices are deployed, the IoT hub starts the peer discovery phase. Each sensor device broadcasts the $P_zD_{control}$ packet once in this configuration. Each device has knowledge about its peers at the completion of the peer discovery phase. The sender id is contained in the $P_zD_{control}$ packet. When a device obtains a $P_zD_{control}$ packet, it checks the peer list for the source device IDs. If the source ID is not yet in the peer list, it must be added; otherwise, the packet will be dropped. If the recipient device's $P_zD_{control}$ packet is set to false, the recipient device sets it to true and broadcasts the $P_zD_{control}$ packet.

The Algorithm 1 explains the above operations. The phase of topology building follows the phase of peer discovery. During this process, each device broadcasts information about its peers to the IoT hub. Each device does this by employing a multicasting approach rather than flooding. The devices begin transmitting peer information to the hub via relay devices. As explained in Algorithm 1, the sender device selects a relay device from $P_z(\alpha)$ and passes peer information to the hub. A sensor device transmits the P_zD_{info} packet just once to avoid network loops. Each device does this by maintaining a list of received peer information. As a result, it lowers network traffic and conserves energy. When the hub receives the P_zD_{info} from the sensor devices, it constructs the peer adjacency matrix. This peer adjacency matrix represents the network structure. The hub determines the cluster heads and the routing paths between them based on the peer adjacency matrix.

Algorithm 1 Peer Discovery

INPUT: Peer Discovery Control Packet

OUTPUT: Return Hub Adjacency Matrix

- 1: $P_z(\alpha) = \phi$ where $P_z(\alpha) = \{ w : w \text{ are the Peer/ Neighbor Device of the device } \alpha \}$;
- 2: $P_zTable(\alpha) = \phi$ where $P_zTable(\alpha)$ is the Peer/ Neighbor table of the IoT Device α ;
- 3: $E_R(\alpha)$ is the remaining energy level of the IoT Device α ;
- 4: Initially $P_zD_{control}(\alpha) = \text{False}$;
- 5: Set $P_zD_{control}(\alpha) = \text{True}$ when the the IoT Device α sends the $P_zD_{control}$ packet;
- 6: $Spot_\alpha$ is the location of the IoT Device α ;
- 7: Device α receives the control packet $P_zD_{control} : \langle P_zD_{control}, ID_\beta, E_R(\beta), Spot_\beta \rangle$ from the Device β ;
- 8: **if** $\beta \notin P_zTable(\alpha)$ **then**
- 9: $P_z(\alpha) = P_z(\alpha) \cup \beta$;
- 10: Update $P_zTable(\alpha)$ with $\langle ID_\beta, E_R(\beta), Spot_\beta \rangle$;
- 11: **if** $P_zD_{control}(\alpha) == \text{false}$ **then**
- 12: $P_zD_{control}(\alpha) \leftarrow \text{True}$;
- 13: Broadcast $P_zD_{control} : \langle P_zD_{control}, ID_\alpha \rangle$; ▷ Broadcast $P_zD_{control}$ packet;
- 14: **else**
- 15: Discard the packet
- 16: **end if**
- 17: Discard the packet
- 18: **end if**
- 19: Device α receives the control packet $P_zD_{info} : \langle P_zD_{info}, P_zTable(\beta), ID_\beta, ID_{relay} \rangle$ from the Device β ;
- 20: **if** $ID_{relay} = ID_\alpha$ **then**
- 21: **if** $\beta \notin P_zD_{info}(\alpha)$ **then**
- 22: $P_zD_{info}(\alpha) = P_zD_{info}(\alpha) \cup \beta$;
- 23: **if** $ID_\alpha == ID_{Hub}$ **then**
- 24: Update peer adjacency matrix using $P_zTable(\beta)$;
- 25: **else**
- 26: Forward the P_zD_{info} packet to the selected relay node;
- 27: **end if**
- 28: Discard the packet
- 29: **end if**

30: Discard the packet
 31: **end if**

4.2. Cluster Head Selection and Cluster Formation

Initially, the energy levels of all devices are equal. The hub computes and tracks the remaining energy of every device after building the peer adjacency matrix. The hub selects CHs in the network based on the following criteria:

1. Two CHs should not be located adjacent to one another.
 Let Device α be selected as CH;
 $P_z(\alpha)$ is a set peer device of the Device α ;
if ($\beta \in P_z(\alpha)$) **then**
 Device β cannot be CH.
end if
2. Each CH's residual energy, $E_R(CH)$, should be larger than the threshold value.
3. Each cluster head should have a peer count of at least $\gamma/2$.

Let k be the number of devices in the network and c denote the ideal number of CHs. Then, $\gamma = (k-c)/c$. In the ideal situation, γ is the average number of devices in a cluster. So each CH should satisfy $P_z(\alpha) \geq \gamma/2$.

After choosing the CH, the hub calculates the path from hub to the CH. The hub checks the peer adjacency matrix and ensures that the selected sensor device's energy level is more than the threshold. Moreover, The routing path's total energy usage should be kept to a minimum. To inform the sensor devices that have been selected as CHs, the hub unicasts the announcement packet ($CH_{announce}$) to the cluster heads through the path determined in Algorithm 2. The $CH_{announce}$ packet then proceeds along the route to the CH. Reverse connections are made by the sensing devices along the way to the CH. A $CH_{announce}$ message causes the CH to send a CH_{ack} acknowledgment packet to the hub. The CH_{ack} packet takes the same way back as the $CH_{announce}$ packet. If the hub does not receive an acknowledgment packet from the CH within a specified time period, it takes a different routing.

Algorithm 2 Cluster Head Announcement

INPUT: Hub sends $CH_{announce}$ packet to the Cluster Heads.

OUTPUT: Cluster Heads send CH_{ack} packet to the hub.

- 1: $Route(k)$ is a collection of sensor devices that form the route between node k and the hub.
- 2: Each relay device maintains a routing table $Realy_{Table}(\alpha)$ with two columns: cluster head id and $next_device$, which is initialized to ϕ .
- 3: Device α receives the $CH_{announce}$ packet from the Device β ;
- 4: $CH_{announce} : < CH_{announce}, Route(CH), ID_{\beta}, ID_{CH} >$
- 5: **if** ($ID_{CH} == ID_{\alpha}$) **then**
- 6: Forward the ACK Packet $CH_{ack} : < CH_{ack}, ID_{\alpha}, next_device >$ towards the hub.
- 7: **else**
- 8: **if** ($\alpha \in Route(CH) \ \&\& \ ID_{CH} \notin Realy_{Table}(\alpha)$) **then**
- 9: Update the $Realy_{Table}(\alpha)$ by updating cluster head id as ID_{CH} and $next_device$ as ID_{β} ;
- 10: Broadcast $CH_{announce} : < CH_{announce}, Route(CH), ID_{\alpha}, ID_{CH} >$ packet.
- 11: **else**
- 12: Discard the packet;
- 13: **end if**
- 14: **end if**
- 15: $CH_{ack} : < CH_{ack}, ID_{\beta}, next_device >$
- 16: **if** ($next_device == ID_{\alpha}$) **then**
- 17: **if** ($ID_{\alpha} == ID_{Hub}$) **then**

```

18:      $Time\_out \leftarrow false;$ 
19:   else
20:     Find the  $next\_device$  of CH  $\beta$  from the  $RealyTable(\alpha)$ ;
21:     Forward the ACK Packet  $CH_{ack} : < CH_{ack}, ID_{\beta}, next\_device >$  towards the hub.
22:   end if
23: else
24:   Drop the packet.
25: end if

```

Afterward, the cluster head broadcasts the CH_{info} advertisement packet to create a cluster as shown in Algorithm 3. The devices that receive several CH_{info} packets pick the cluster head based on the RSSI value that is the highest RSSI. After the CH selection, a device sends the CH_{join} packet with the joining request. Each interested device sends an equivalent CH_{join} packet to the cluster head. Following receipt of all joining requests, the cluster head broadcasts information to the hub about each cluster member. The CH utilizes Time Division Multiple Access (TDMA) to create a time-slot schedule for the cluster members and distributes it to them to alleviate congestion. This TDMA slot can be used to maintain collision-free communication among the CHs and CMs.

Algorithm 3 Cluster Formation

INPUT: CH sends CH_{info} packet to the CMs.

OUTPUT: CH sends $Cluster_member(CH)$ to the hub and TDMA slots to each CM.

```

1: Device  $\alpha$  receives the  $CH_{info}$  packet from the Device  $\beta$ , where  $\beta \in CH$ 
2:  $CH_{info} : < CH_{info}, ID_{\beta} >$ 
3: Device  $\alpha$  selects the CH with the maximum received signal intensity as its CH after receiving all  $CH_{info}$  packets.
4: Device  $\alpha$  sends the  $CH_{join}$  packet to the selected CH.
5: Device  $\alpha$  receives the  $CH_{join}$  packet from the Device  $\beta$ , where  $\alpha \in CH$ 
6:  $CH_{join} : < CH_{join}, ID_{\beta}, ID_{CH} >$ 
7: if ( $ID_{\alpha} == ID_{CH}$ ) then
8:    $Cluster\_member(\alpha) \leftarrow Cluster\_member(\alpha) \cup \beta;$ 
9:   Device  $\alpha$  sends the  $Cluster\_member(\alpha)$  to the hub after receiving all the  $CH_{join}$  packets.
10:  Device  $\alpha$  sends the TDMA slots to each CM.
11: else
12:  Discard the packet.
13: end if

```

Lemma 1. The clustering process needs the transmission of $\mathcal{O}(\alpha)$ control messages, where α is the number of sensor devices in the network.

Proof. Each device begins the cluster formation process by broadcasting a $P_z D_{control}$ packet. Thus, the network contains α messages. Each device communicates information about its peers to the hub, which accepts α messages again. To join the cluster head, every cluster member broadcasts a CH_{join} packet. Assume that the number of cluster heads created is β . Thus, the total number of join requests is $(\alpha - \beta)$, and the cluster heads require β messages for each time slot. Thus, in cluster formation, the total number of control messages required is $\alpha + (\alpha - \beta) + \beta + \beta = 2\alpha + \beta$. As a result, the overall complexity of the control message throughout the cluster formation network is $\mathcal{O}(\alpha)$. \square

Lemma 2. The network's total energy usage is $E_{Total} = \sum((E_{ch} \times \beta + E_{cm} \times (\alpha - \beta)))$.

Proof. Each device in CRPSH is classified as a cluster head or a cluster member. Cluster members transmit data to the CH, which collects and delivers the data to the hub. The transmission, receipt, and aggregation of data by the each cluster head requires

E_{ch} energy. Each cluster member uses E_{cm} energy during transmission, reception, and sleep. If the number of CHs in the network is β , then the network's total energy usage is $E_{Total} = \sum((E_{ch} \times \beta + E_{cm} \times (\alpha - \beta)))$. \square

4.3. Data Transmission

Within the specified time, the cluster member transmits the sensed data to the CH and then enters sleep mode. In the subsequent time slot, the sensor device reactivates to transmit the data. As a result, the protocol optimizes the energy efficiency of the sensor devices. The CH collects data and transmits it to the hub via the specified path. The CH receives an acknowledgment packet when the data arrives at the hub. The data is re-transmitted if the CH does not receive confirmation from the hub. Because the hub contains all of the network's topological information, it continuously monitors each device's remaining energy. If the hub detects that a device's residual energy is less than the predefined threshold, it redirects the CH to another available path.

4.4. Re-Clustering and Rerouting

The hub continually monitors each device's remaining energy to ensure that the load is distributed evenly among the devices. If a device's energy level falls below the threshold, the hub begins re-clustering or rerouting according to the role of the device. If the device is a relay device for any path, the hub chooses another way to bypass it. If the device is a CH, the hub switches to a different CH and path. This approach extends the network's life. If a device has less residual energy than the threshold, it does not participate in routing or becoming a CH but instead functions as a cluster member.

5. Simulation Results

The complete set of simulations is carried out using Castalia simulator. Table 2 shows the parameters used for simulation.

Table 2. Simulation Parameters.

Parameter Name	Value
Network Size	100 × 100 m ²
Number of sensor devices	100
Data packet size	512 bytes
Control packet size	32 bytes
Initial energy	1 J
E_{Embb}	50 nJ/bit
E_{fs}	10 pJ/bit/m ²
E_{mp}	0.0013 pJ/bit/m ⁴
d_0	87 m
E_{Comp}	5 nJ/bit
E_{low}	0.2 nJ/s
Simulation time	400 s
MAC protocol	TMAC

5.1. Average Energy Consumption

The average energy consumption for each protocol is depicted in Figure 1. It is observed that the proposed protocol (CRPSH) has a lower control packet overhead than PCMRP and REDCL. The proposed scheme does not employ flooding and does not involve the entire network in selecting CHs and multipaths. The hub selects the CHs and routing paths on its own. PCMRP, on the other hand, creates a multipath by flooding control packets across the network. This is a significant contributor to the increase in control packet overhead. Additionally, the multipath is reconstructed if any device becomes the source. This adds to the protocol's overhead. PCMRP transmits data via the shortest path possible. However, because of the increased overhead associated with control packets, the average energy consumption is higher.

The efficiency of the routing protocol relies on energy consumption. The smaller the network energy consumption, the greater the network lifetime. Therefore, it is the total energy consumed by IoT devices to perform transmission, reception, processing, and sleeping activities. The REDCL method prioritizes the selection of a smaller number of active reporting nodes (ARNs) in hotspot areas over the selection of more ARNs in nonhotspot areas. The REDCL method converges the paths of several ARNs monitoring an event outside of nonhotspot zones and sends them to the hub after data aggregation. The hotspot area's ARNs are unable to transfer data directly to the hub. They must communicate with the hub through nonhotspot ARNs. This in turn places an additional burden on nonhotspot ARNs. As a result, the energy consumption of nonhotspot ARNs is rather high, therefore increasing the overall energy consumption of the network.

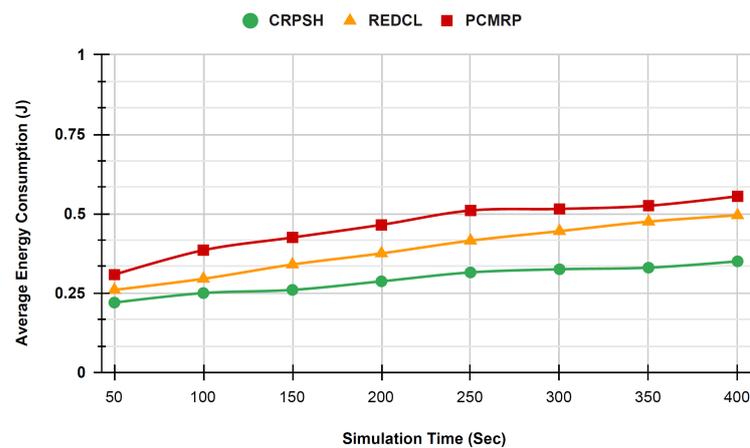


Figure 1. Average Energy Consumption.

5.2. Average End-to-End Delay

It is calculated as the time it takes for a data packet to be generated at the source and received successfully at the sink. Each potential cluster head in the PPCMP must wait before becoming the cluster head. Furthermore, when the source node changes, the protocol must recreate the multipath for the new source node for each new event. This increases the protocol's total latency. The REDCL approach sends data packets to the principal route based on a single event. It collects data before sending it to the hub, which causes packet delivery to be delayed. CRPSH, on the other hand, allows for various pathways to be taken. The proposed protocol has a more reduced end-to-end latency than PCMRP and REDCL, as shown in Figure 2.

Conversely, for CRPSH, multiple paths are available. The result in Figure 2 indicates that the proposed protocol's end-to-end latency is less than that of PCMRP and REDCL.

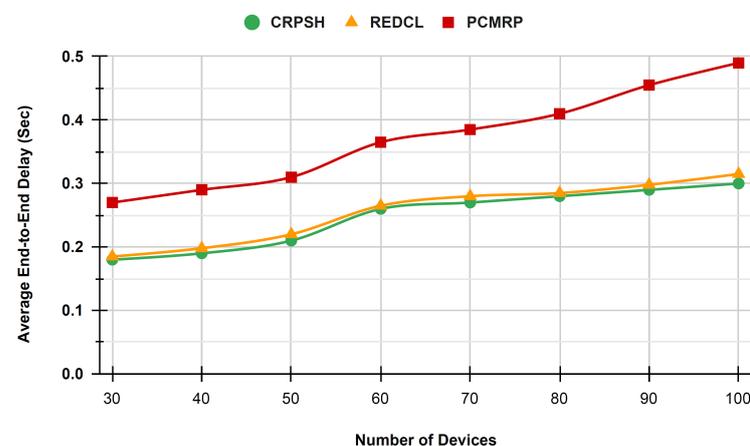


Figure 2. Average End-to-End Delay.

5.3. Packet Delivery Ratio

It is defined as the ratio of IoT hub receipt data packets to data packets sent by the source. For each protocol, the packet delivery ratio is illustrated in the Figure 3. PCMRP employs node-disjoint multipath routing, that improves reliability and, as a result, the delivery ratio. The REDCL method aggregates data by converging multiple routes of event monitoring devices into a single route. As a result, its packet delivery ratio is more than that of PCMRP. However, under the proposed approach (CRPSH), the hub picks the path and keeps track of each device's remaining energy. When it detects that a device's remaining energy is less than the threshold, it switches to a different path for data transmission. As a result, data loss is minimal.

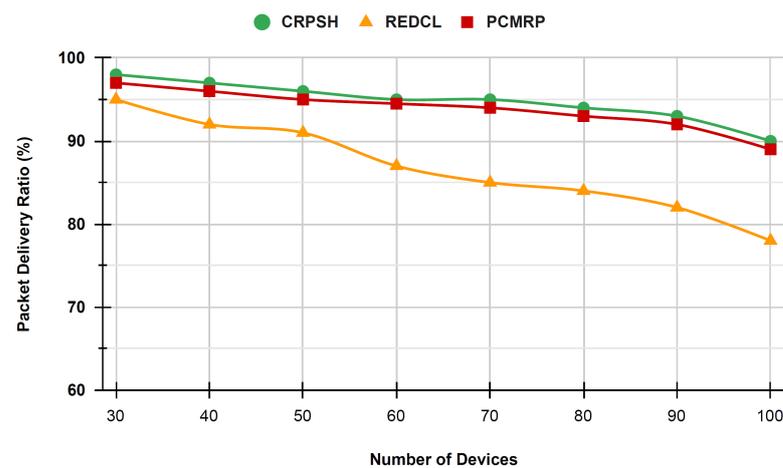


Figure 3. Packet Delivery Ratio.

5.4. Network Lifetime

It is the time duration where the network works perfectly. For each protocol, the network lifetime is illustrated in the Figure 4. The proposed approach clearly outperforms the REDCL and PPCMP in terms of network lifetime. This is because it uses fewer control packets and distributes the workload properly across all the sensor devices.

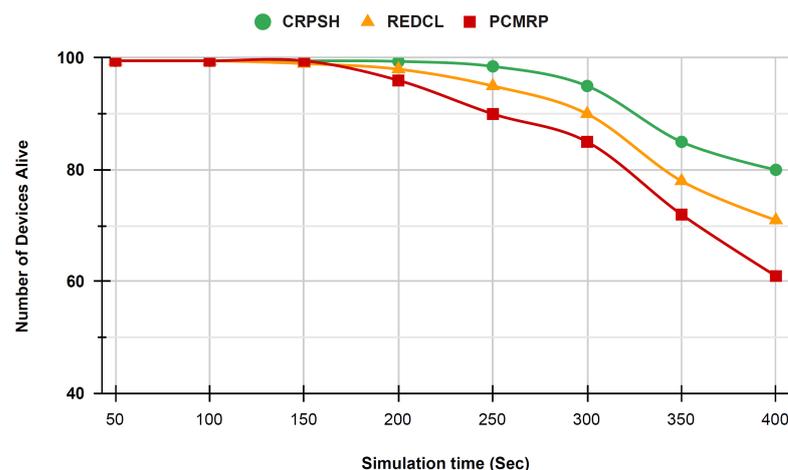


Figure 4. Network Lifetime.

6. Conclusions

This paper proposed a Cluster-based Routing Protocol with Static Hub (CRPSH) for WSN-assisted IoT networks. Sensor devices are often densely distributed across the network, and a monitoring zone may be covered by many sensor devices, resulting in redundant data. In CRPSH, we have used the clustering technique to reduce the dupli-

cate data. CRPSH lowers the burden on the regular sensor devices and assigns more responsibilities such as clustering, route selection, and energy management to the hub.

The network reliability is the main concern for the existing routing protocols. In CRPSH, the multipath approach increases the proposed protocol's reliability. Correspondingly, we compared CRPSH's performance to existing models, such as PCMRP and REDCL, and discovered that CRPSH is energy efficient and extends the network's lifetime and packet delivery ratio.

However, CRPSH often suffers from hotspot problems. The devices closer to the hub drain their energy at a faster rate compared with other devices (devices located at a far distance from the hub) as they have to perform more communication, and hence the whole network may become detached or isolated. A mobile hub is a possible solution to the hotspot problem.

Author Contributions: Conceptualization, R.K.L.; methodology, H.M.; software, F.A.-T.; validation, C.A.; formal analysis, R.K.L., M.K.; investigation, H.M.; resources, F.A.-T., M.K.; data curation, C.A.; writing—original draft preparation, R.K.L.; writing—review and editing, H.M.; visualization, F.A.-T.; supervision, H.M.; project administration, F.A.-T.; funding acquisition, C.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CH	Cluster Heads
CM	Cluster Members
LLNs	Low-power and Lossy networks
CRPSH	Cluster-based Routing Protocol with Static Hub
IoT	Internet of Things
ANPIREQ	AN Position Information Request packet
ANPIRES	AN Location Information Response
QDD	Quadtree-based Routing Protocol
CBRP	Centroid-based Routing Protocol
SCBC	Sector-Chain-Based Clustering Routing Protocol
SCH	Secondary Cluster Head
BS	Base Station
HRPM	Hierarchical Rendezvous Point Multicast
HGMR	Hierarchical Geographic Multicast Routing Protocol
GMCAR	Grid-based Multipath Routing Protocol
LGH	Local Grid Head
TDMA	Time Division Multiple Access
GBRR	Grid-Based Reliable Routing
MSGR	Grid-Based Sustainable Routing Protocol
PCMRP	Passive cluster-based multipath routing protocol for WSNs
REDCL	Reliable and energy-efficient data collection for WSNs
E_{Embb}	Energy required for an embedded circuit to receive or transmit a signal of one bit
E_{Amp}	Amplifier energy consumption to preserve radio reliable transmission

References

1. Sarkar, S.; Debnath, A. Green IoT: Design Goals, Challenges and Energy Solutions. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 8–10 July 2021; pp. 637–642.
2. Verma, G.; Prakash, S. A Comparative Study Based on Different Energy Saving Mechanisms Based on Green Internet of Things (GIoT). In Proceedings of the 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 4–5 June 2020; pp. 659–666.
3. Al-Turjman, F.M.; Zahmatkesh, H.; Shahroze, R. An overview of security and privacy in smart cities' IoT communications. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3677. [[CrossRef](#)]
4. Deebak, B.D.; Al-Turjman, F.M. Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Gener. Comput. Syst.* **2021**, *116*, 406–425. [[CrossRef](#)]
5. Lenka, R.K.; Rath, A.K.; Sharma, S. Building Reliable Routing Infrastructure for Green IoT Network. *IEEE Access* **2019**, *7*, 129892–129909. [[CrossRef](#)]
6. Lenka, R.K.; Rath, A.K.; Tan, Z.; Sharma, S.; Puthal, D.; Simha, N.V.R.; Prasad, M.; Raja, R.; Tripathi, S.S. Building Scalable Cyber-Physical-Social Networking Infrastructure Using IoT and Low Power Sensors. *IEEE Access* **2018**, *6*, 30162–30173. [[CrossRef](#)]
7. Sourailidis, D.; Koutsiamanis, R.A.; Papadopoulos, G.Z.; Barthel, D.; Montavont, N. RFC 6550: On Minimizing the Control Plane Traffic of RPL-based Industrial Networks. In Proceedings of the 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Cork, Ireland, 31 August–3 September 2020; pp. 439–444.
8. Al-Turjman, F.; Deebak, B.D. Seamless Authentication: For IoT-Big Data Technologies in Smart Industrial Application Systems. *IEEE Trans. Ind. Informatics* **2021**, *17*, 2919–2927. [[CrossRef](#)]
9. Al-Turjman, F.; Altrjman, C.; Din, S.; Paul, A. Energy monitoring in IoT-based ad hoc networks: An overview. *Comput. Electr. Eng.* **2019**, *76*, 133–142. [[CrossRef](#)]
10. Mohapatra, K.; Lenka, R.K.; Sharma, S. A Survey on Classical and Optimized Hierarchical Routing Protocols for IoT and WSN. In Proceedings of the 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 7–9 October 2021; pp. 620–624.
11. Pratik, T.; Lenka, R.K.; Nayak, G.K.; Kumar, A. An Architecture to Support Interoperability in IoT Devices. In Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018; pp. 705–710.
12. Lenka, R.K.; Barik, R.K.; Das, N.K.; Agarwal, K.; Mohanty, D.; Vipsita, S. PSPS: An IoT based predictive smart parking system. In Proceedings of the 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), Mathura, India, 26–28 October 2017; pp. 311–317.
13. Lenka, R.K.; Aggarwal, A.; Rath, A.; Sharma, S. Cluster-based rendezvous routing protocol for wireless sensor network. In Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 5–6 May 2017; pp. 748–752.
14. Lenka, R.K.; Rath, A.K.; Sharma, S. Routing Protocols in WSN Assisted IoT Infrastructure—A Review. In Proceedings of the 2019 International Conference on Intelligent Computing and Remote Sensing (ICICRS), Bhubaneswar, India, 19–20 July 2019; pp. 1–6.
15. Liu, X. Atypical hierarchical routing protocols for wireless sensor networks: A review. *IEEE Sens. J.* **2015**, *15*, 5372–5383. [[CrossRef](#)]
16. Natarajan, Y.; Srihari, K.; Dhiman, G.; Chandragandhi, S.; Gheisari, M.; Liu, Y.; Lee, C.C.; Singh, K.K.; Yadav, K.; Alharbi, H.F. An IoT and machine learning-based routing protocol for reconfigurable engineering application. *IET Commun.* **2022**, *16*, 464–475. [[CrossRef](#)]
17. Sood, T.; Sharma, K. P-LUET: A Prolong Lines of Uniformity Based Enhanced Threshold Algorithm for Heterogeneous Wireless Sensor Network Enabled Internet of Things Framework. *Wirel. Pers. Commun.* **2021**, *120*, 2935–2970. [[CrossRef](#)]
18. Rahman, G.M.E.; Wahid, K.A. LDCA: Lightweight Dynamic Clustering Algorithm for IoT-Connected Wide-Area WSN and Mobile Data Sink Using LoRa. *IEEE Internet Things J.* **2022**, *9*, 1313–1325. [[CrossRef](#)]
19. Karthick, K.; Asokan, R. Mobility Aware Quality Enhanced Cluster Based Routing Protocol for Mobile Ad-Hoc Networks Using Hybrid Optimization Algorithm. *Wirel. Pers. Commun.* **2021**, *119*, 3063–3087. [[CrossRef](#)]
20. Shi, K.; Liu, C.; Sun, Z.; Yue, X. Coupled orbit-attitude dynamics and trajectory tracking control for spacecraft electromagnetic docking. *Appl. Math. Model.* **2022**, *101*, 553–572. [[CrossRef](#)]
21. Hamida, E.B.; Chelius, G. A line-based data dissemination protocol for wireless sensor networks with mobile sink. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 2201–2205.
22. Mohapatra, H.; Rath, A.K. IoE based framework for smart agriculture. *J. Ambient Intell. Humaniz. Comput.* **2022**, *13*, 407–424. [[CrossRef](#)]
23. Mohapatra, H.; Rath, A.K. An IoT based efficient multi-objective real-time smart parking system. *Int. J. Sens. Netw.* **2021**, *37*, 219–232. [[CrossRef](#)]
24. Mohapatra, H.; Rath, A.K. A fault tolerant routing scheme for advanced metering infrastructure: An approach towards smart grid. *Clust. Comput.* **2021**, *24*, 2193–2211. [[CrossRef](#)]
25. Tunca, C.; Isik, S.; Donmez, M.Y.; Ersoy, C. Ring routing: An energy-efficient routing protocol for wireless sensor networks with a mobile sink. *IEEE Trans. Mob. Comput.* **2014**, *14*, 1947–1960. [[CrossRef](#)]

26. Shin, J.H.; Kim, J.; Park, K.; Park, D. Railroad: Virtual infrastructure for data dissemination in wireless sensor networks. In Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, Montreal, QC, Canada, 10–13 October 2005; pp. 168–174.
27. Sharma, S.; Puthal, D.; Jena, S.K.; Zomaya, A.Y.; Ranjan, R. Rendezvous based routing protocol for wireless sensor networks with mobile sink. *J. Supercomput.* **2017**, *73*, 1168–1188. [[CrossRef](#)]
28. Mir, Z.H.; Ko, Y.B. A quadtree-based data dissemination protocol for wireless sensor networks with mobile sinks. In Proceedings of the IFIP International Conference on Personal Wireless Communications, Albacete, Spain, 20–22 September 2006; Springer: Berlin/Heidelberg, Germany, 2006; pp. 447–458.
29. Shen, J.; Wang, A.; Wang, C.; Hung, P.C.; Lai, C.F. An efficient centroid-based routing protocol for energy management in WSN-assisted IoT. *IEEE Access* **2017**, *5*, 18469–18479. [[CrossRef](#)]
30. Tan, N.D.; Viet, N.D. SCBC: Sector-chain based clustering routing protocol for energy efficiency in heterogeneous wireless sensor network. In Proceedings of the 2015 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 14–16 October 2015; pp. 314–319.
31. Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H. An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **2002**, *1*, 660–670. [[CrossRef](#)]
32. Gnanambigai, J.; Rengarajan, D.N.; Anbukkarasi, K. Leach and its descendant protocols: A survey. *Int. J. Commun. Comput. Technol.* **2012**, *1*, 15–21.
33. Biradar, R.V.; Sawant, S.; Mudholkar, R.; Patil, V. Multihop routing in self-organizing wireless sensor networks. *Int. J. Comput. Sci. Issues* **2011**, *8*, 155.
34. Qiang, T.; Bingwen, W.; Zhicheng, D. MS-Leach: A routing protocol combining multi-hop transmissions and single-hop transmissions. In Proceedings of the 2009 Pacific-Asia Conference on Circuits, Communications and Systems, Chengdu, China, 16–17 May 2009; pp. 107–110.
35. Farooq, M.O.; Dogar, A.B.; Shah, G.A. MR-LEACH: Multi-hop routing with low energy adaptive clustering hierarchy. In Proceedings of the 2010 Fourth International Conference on Sensor Technologies and Applications, Venice, Italy, 18–25 July 2010; pp. 262–268.
36. Sanchez, J.A.; Ruiz, P.M.; Stojmenovic, I. GMR: Geographic multicast routing for wireless sensor networks. In Proceedings of the 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Reston, VA, USA, 28 September 2006; Volume 1, pp. 20–29.
37. Buttyán, L.; Schaffer, P. Position-based aggregator node election in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2010**, *6*, 679205. [[CrossRef](#)]
38. Akl, R.; Sawant, U. Grid-based coordinated routing in wireless sensor networks. In Proceedings of the 2007 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 11–13 January 2007; pp. 860–864.
39. Das, S.M.; Pucha, H.; Hu, Y.C. Distributed hashing for scalable multicast in wireless ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.* **2008**, *19*, 347–362. [[CrossRef](#)]
40. Koutsonikolas, D.; Das, S.M.; Hu, Y.C.; Stojmenovic, I. Hierarchical geographic multicast routing for wireless sensor networks. *Wirel. Netw.* **2010**, *16*, 449–466. [[CrossRef](#)]
41. Banimelhem, O.; Khasawneh, S. GMCAR: Grid-based multipath with congestion avoidance routing protocol in wireless sensor networks. *Ad Hoc Netw.* **2012**, *10*, 1346–1361. [[CrossRef](#)]
42. Chi, Y.P.; Chang, H.P. An energy-aware grid-based routing scheme for wireless sensor networks. *Telecommun. Syst.* **2013**, *54*, 405–415. [[CrossRef](#)]
43. Khan, A.W.; Abdullah, A.H.; Razzaque, M.A.; Bangash, J.I. VGDR: A virtual grid-based dynamic routes adjustment scheme for mobile sink-based wireless sensor networks. *IEEE Sens. J.* **2014**, *15*, 526–534. [[CrossRef](#)]
44. Jin, R.C.; Gao, T.; Song, J.Y.; Zou, J.Y.; Wang, L.D. Passive cluster-based multipath routing protocol for wireless sensor networks. *Wirel. Netw.* **2013**, *19*, 1851–1866. [[CrossRef](#)]
45. Dong, M.; Ota, K.; Liu, A. RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks. *IEEE Internet Things J.* **2016**, *3*, 511–519. [[CrossRef](#)]
46. Sharma, S.; Suresh, D. VGBST: A virtual grid-based backbone structure type scheme for mobile sink based wireless sensor networks. In Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015), Unnao, India, 6–7 March 2015; pp. 1–5.
47. Meng, X.; Shi, X.; Wang, Z.; Wu, S.; Li, C. A grid-based reliable routing protocol for wireless sensor networks with randomly distributed clusters. *Ad Hoc Netw.* **2016**, *51*, 47–61. [[CrossRef](#)]
48. Sharma, S.; Puthal, D.; Tazeen, S.; Prasad, M.; Zomaya, A.Y. MSGR: A mode-switched grid-based sustainable routing protocol for wireless sensor networks. *IEEE Access* **2017**, *5*, 19864–19875. [[CrossRef](#)]
49. Jung, S.M.; Han, Y.J.; Chung, T.M. The concentric clustering scheme for efficient energy consumption in the PEGASIS. In Proceedings of the 9th International Conference on Advanced Communication Technology, Gangwon, Korea, 12–14 February 2007; Volume 1, pp. 260–265.
50. Xi-rong, B.; Shi, Z.; Ding-yu, X.; Zhi-tao, Q. An energy-balanced chain-cluster routing protocol for wireless sensor networks. In Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 24–25 April 2010; Volume 2, pp. 79–84.

51. Lindsey, S.; Raghavendra, C.; Sivalingam, K.M. Data gathering algorithms in sensor networks using energy metrics. *IEEE Trans. Parallel Distrib. Syst.* **2002**, *13*, 924–935. [[CrossRef](#)]
52. Chen, K.H.; Huang, J.M.; Hsiao, C.C. CHIRON: An energy-efficient chain-based hierarchical routing protocol in wireless sensor networks. In Proceedings of the 2009 Wireless Telecommunications Symposium, Prague, Czech Republic, 22–24 April 2009; pp. 1–5.
53. Kim, H.S.; Han, K.J. A power efficient routing protocol based on balanced tree in wireless sensor networks. In Proceedings of the First International Conference on Distributed Frameworks for Multimedia Applications, Besancon, France, 6–9 February 2005; pp. 138–143.
54. Ding, M.; Cheng, X.; Xue, G. Aggregation tree construction in sensor networks. In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484), Orlando, FL, USA, 6–9 October 2003; Volume 4, pp. 2168–2172.
55. Tan, H.Ö.; Körpeoğlu, I. Power efficient data gathering and aggregation in wireless sensor networks. *Acm Sigmod Rec.* **2003**, *32*, 66–71. [[CrossRef](#)]
56. Qiu, W.; Skafidas, E.; Hao, P. Enhanced tree routing for wireless sensor networks. *Ad Hoc Netw.* **2009**, *7*, 638–650. [[CrossRef](#)]
57. Luo, H.; Ye, F.; Cheng, J.; Lu, S.; Zhang, L. TTDD: Two-tier data dissemination in large-scale wireless sensor networks. *Wirel. Netw.* **2005**, *11*, 161–175. [[CrossRef](#)]
58. Mo, H.S.; Lee, E.; Park, S.; Kim, S.H. Virtual line-based data dissemination for mobile sink groups in wireless sensor networks. *IEEE Commun. Lett.* **2013**, *17*, 1864–1867. [[CrossRef](#)]
59. Roy, N.R.; Chandra, P. Energy dissipation model for wireless sensor networks: A survey. *Int. J. Inf. Technol.* **2020**, *12*, 1343–1353. [[CrossRef](#)]