EAI Endorsed Transactions
on Scalable Information Systems Research Article **EAI.EU**

IoT Protocols: Connecting Devices in Smart Environments

Teeb Hussein Hadi[1,*]

[1]Information Technology Management Department, Technical College of Management, Middle Technical University, Baghdad, Iraq

Abstract

The study delves into the implications of various IoT protocols on communication efficiency and energy consumption within smart environments. The RVRR (routing via respective reducer) protocol emerges as a standout performer, showcasing notable advantages over other conventional protocols. Specifically, the results demonstrate a substantial reduction in communication costs with RVRR, exhibiting improvements of 22.72%, 43.46%, and 49.04% when compared to ILP, SDN-Smart, and R-Drain, respectively. excels in data transmission, achieving commendable reductions in Round-Trip Time (RTT) and enhancing overall energy efficiency. It registers an 18.80% decrease in energy consumption compared to ILP, 28.65% compared to SDN-Smart, and a significant 37% reduction when compared to R-Drain. This suggests that RVRR is adept at optimizing resource usage (routing via respective reducer) and minimizing energy consumption, crucial aspects in the context of IoT applications. The study reveals that RVRR contributes to an extended network lifespan, outperforming other protocols by substantial margins. It showcases a 19.45% improvement over ILP, 39.16% over SDN-Smart, and an impressive 54.60% over R-Drain. This underscores the sustainability and longevity benefits offered by RVRR (routing via respective reducer), making it a promising protocol for efficient and enduring IoT applications within smart environments.

Keywords: Communication Efficiency, Energy Consumption, IoT Protocols, RVRR Protocol, Smart Environments

Received on 06 April 2024, accepted on 25 April 2024, published on 26 April 2024

doi: 10.4108/eetsis.5665

1. Introduction

In order to perform in-network processing, a software-defined framework is integrated in this study, offering a method for sensibly preserving the energy of sensor nodes. The SDN controller selects reducers from inside the network nodes [1]. Following that, the control parcels are sent through the familiar way and the information bundles are sent by means of the in-network handling way utilizing the proposed steering convention, RVRR, as per the minimizer choice. The lifetime of the introduced network is reached out because of this striking decrease in correspondence costs [2]. Smart environments, which seamlessly blend the digital and physical worlds, are being shaped by the fast development of Internet of Things (IoT) technology. IoT protocols, which operate as the communication foundation that makes it possible for devices to interact and share data effectively, are crucial to this paradigm shift. Interoperability, security, and scalability are critical requirements for IoT protocols, and they will become more and more so as the quantity and variety of connected devices increase [3]. To all the more likely comprehend the mind-boggling universe of IoT conventions and their job in advancing the association that controls the dynamic and keen activity of shrewd conditions, this presentation lays the foundation.

1.1. Background

The core of the loT, the sensor network, generates a massive amount of data that is erratic and is a significant source of big data. As a result, developing infrastructure that can handle large data presents serious issues for organizations.

---

[*] Corresponding author. Email: eng.teebhussien@mtu.edu.iq,

A CISCO study states that each day, sensors produce five Quintilian data bytes. Additionally, according to an IDC estimate, sensors would generate 79.4 zettabytes (ZB) of data by 2025. Consequently, it is discovered that in-network processing—which involves lowering the amount of data before sending it to the cloud—is crucial. Moreover, the load on the small sensor nodes will be reduced by processing data prior to its transfer to the sink node [4]. As a result, the network's overall communication costs are significantly reduced. Better real-time performance is made possible by the resulting decrease in network latency caused by this lower communication cost.

Suitable hubs are chosen as minimizers from a pool of haphazardly distributed hubs all through the organization to complete in-network handling. At the point when a hub is assigned as a minimizer in a performing various tasks climate, any remaining hubs in the organization that distinguish a similar work will move the information towards that minimizer, consequently disturbing the transmission capacity limitation. Too far, a large number of academics have optimized the CH selection process in WSN using game theory to increase decision-making efficiency. Recurring games are a significant class of dynamic games that recur over time and adjust their strategy based on past player behaviors. The utility function of repeated games—which the sensor nodes aim to maximize—has been formulated in the section that follows. To pick reducers efficiently, the SDN controller plays the game. Every minimizer communicates the resultant information to the sink hub in the wake of executing minimizer capabilities that are progressively stacked into it, normally saving the organization energy. For this work, the main contributions are:

- A routing technique that sends packets to the sink node via the appropriate reducer has been devised based on the reducer selection;
- Extensive simulation-based tests show that the RVRR (routing via respective reducer) protocol is successful in lowering total communication costs, which minimizes nodes' energy usage.

1.2. The Ubiquitous Network: Exploring the Internet of Things (IoT)

Imagine living in a future where your automobile predicts traffic jams before you ever get on the road, your thermostat adjusts to your daily routine, and your refrigerator reorders food when they run low. This is the fact that the Internet of Things, or IoT, is quietly integrating into our daily lives by joining commonplace items to a wide-ranging digital network.

The Internet of Things (IoT) is based on the straightforward idea of integrating microchips, sensors, and actuators into commonplace objects to enable data exchange and communication via the network. These gadgets, which may be anything from wearable and smart light bulbs to industrial gear and agricultural sensors, integrate into a greater ecosystem and communicate with one another and the outside world in real time.

Not only a futuristic gimmick, this connection is drastically changing the way we work, live, and engage with the world. IoT technologies provide ease and customized comfort in our homes by automatically modifying the lighting, temperature, and entertainment according to our preferences. Dishwashing and laundry are made easier by linked appliances, while safety is improved by smart cameras and security systems.

The Internet of Things is transforming a variety of businesses beyond the home, including manufacturing and healthcare. Medical equipment that are connected can remotely monitor patients in hospitals, resulting in better care and the ability to identify health problems early on. Sensors built into machinery in factories improve operating efficiency, forecast maintenance requirements, and optimize manufacturing processes [5].

The influence of the IoT stretches much deeper, altering our infrastructure and cities. By adjusting to actual traffic patterns, smart traffic lights save pollution and congestion. Environmental sensors monitor air and water quality, giving data for informed decision-making and pollution management. Waste management systems that are networked maximize collection routes and encourage sustainability [6].

However, enormous power also entails considerable responsibility. Significant questions concerning data ownership, security, and privacy are brought up by the IoT's broad use. Ensuring the safety and ethical use of personal data becomes increasingly important as more gadgets gather and exchange information. To successfully traverse this networked environment, we require strong security protocols and unambiguous ethical standards.

The Internet of Things has immense promise, despite these obstacles. With the growth of the network and advancements in technology, the prospects appear limitless [7]. Imagine self-driving automobiles that effortlessly navigate smart cities, precision agriculture that maximizes produce while minimizing environmental impact, or personalized learning environments that are tailored to individual students.

Though there is still a long way to go before the Internet of Things becomes really pervasive, the groundwork for a revolutionary future has already been laid. By carefully examining the potential and tackling the obstacles, we can leverage the linked world's capacity to create a more intelligent, secure, and sustainable future for all.

1.3. System Model

We think about a commonplace SDWSN (Software-Defined Wireless Sensor Network) plan, which comprises of an assortment of sensor hubs, N = {n1, n2..., nm}, where m is the quantity of sensor hubs, and a sensibly incorporated regulator. Likewise, with the SDN worldview, there is an unmistakable partition between the framework layer and control layer. All the more exactly, the sink node(s) and sensor hubs, which handle in-network handling and bundle sending, make up the foundation layer. The remote-working SDN regulator is housed in the control layer. The organization geography, which is addressed as G= (N, L) in which N is the arrangement of programmable sensor hubs organized on the checking district and L is the arrangement of every coordinated connection, is surely known by the SDN regulator.

As found in Figure 1, sensor hubs are introduced with different sorts of sensors, including tension, temperature, and moistness. Let Si ∈ [l, S] address the sensor type recognizable proof. Hubs ni and ni+I are quick neighbours of an association li ∈ L. The hubs ni and ni+I are supposed to never have a similar work si relegated to them (sensor type and sensor task are utilized conversely in this work and are meant by the documentation si). Pis is the probability that the sensor hub ni has a sensor Si.

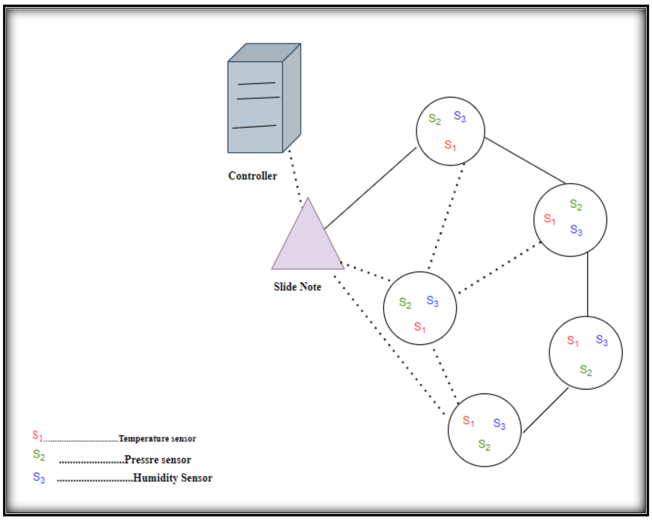


Figure 1: An illustration of multitasking in SDWSN

Prior to forwarding, the data produced by the sensors are converted into key-value pairs, < s, v >. Each type of sensor will have a single reducer., i.e., $\sum_{j=1}^{m} r_{js} = 1 \, \forall_{s,}$ where r_{js} is a binary variable that carries the value O otherwise and 1 whenever the node nJ operates as a reducer for sensor type si. This may be shown in this manner:

$$r_{js} = \begin{cases} 1, & \text{if node } n_j \text{ erduces sensor type } s_{i,} \\ 0, & \text{otherwise.} \end{cases} \tag{1.1}$$

As a result, nodes that produce data for a specific task have to send the data to the appropriate reducer. It is necessary to guarantee the minimum sensing rate in order to guarantee the accuracy of sensing for a given task. ns ⊆ N sensor nodes need to execute the task. The subset of sensor nodes is represented by ns at time slot τ. Si. Every node n ∈ ns is considered a relay node for the purpose of sending data packets to the relevant reducer [8]. The regulator powers the lessening capability on the minimizers after they are picked, considering the memory limit of the sensor hubs. As a result, multiple platforms enable simultaneous computation and communication on sensor nodes.

A crucial matter that requires extra attention in SDWSNs with dynamic topology changes is reducer selection. Furthermore, the sensor task, si, is started at time instance τ in a number of network-wide nodes. Thus, the following area forms the issue of picking the minimizers for every sensor type si ∈ S.

2. Literature Review

Shen, Y., Zhang, T., Wang, Y., Wang, H., & Jiang, X. (2017) The Internet of Things (IoT) has significantly impacted daily life through various protocols [9]. A general IoT architecture, inspired by the Internet, allows for diverse devices to be easily accessible and operated through network DIY for data aggregation and application DIY for service collaboration. This architecture supports a centralized controller, enabling on-demand device interoperability and a consistent microworld.

Zhang, Y., Shen, Y., Wang, H., Yong, J., & Jiang, X. (2015) This article uses physical layer security to investigate the secrecy outage performance of wireless communications under eavesdropper cooperation [10]. It employs traditional Probability Theory to assess non-colluding situations and the Cauchy Integral Theorem, Laplace transform, and keyhole contour integral to study dangerous M-colluding scenarios. The signal-to-interference ratio rises both super linearly and sub linearly with M, according to simulation and numerical data.

Wang, H., Zhang, Z., & Taleb, T. (2018) The assessment of the literature delves into the security and privacy issues surrounding Internet of Things (IoT) systems, highlighting the necessity of strong security protocols and processes that protect privacy [11]. In addition, it looks at new approaches and technologies that improve IoT security and privacy, providing ideas for further study and development.

Lakshmi, M. S., Kashyap, K. J., Khan, (2023) Farm disease detection is difficult since individual plant monitoring is time-consuming. Accurate disease forecasts are produced with the application of AI and Deep Learning (DL). IoT-enabled smart farming maximizes current practices for higher output and efficiency [12]. Since rice is a staple food, it's critical to use automated methods and Internet of Things sensors for early illness identification. AI has shown effective in the diagnosis and treatment of plant illnesses when applied to the WO-DRL model, which was trained on images of rice leaves.

Zhu, X., Hu, C., Lu, Y., Wang, Z., & Xue, H. (2023) Due to the electricity system's heavy reliance on electronic data processing and transmission, strict security measures are needed. The growth of Internet technology has made it possible to apply it to more sectors, necessitating the intelligent administration of the whole communication infrastructure [13]. Strong Internet of Things technology enhances overall security by combining processing and information transmission channels. In order to power the Internet of Things, this article presents the Bayesian network method and examines lightweight encryption implementation. It compares and demonstrates the efficacy of.

3. Proposed Methodology

The proposed work chooses reducers in the infrastructure layer that perform in-network processing in order to create an energy-efficient routing protocol for SDWSN. The RVRR routing protocol, which uses the shortest path to forward control packets to the sink node and data packets to the appropriate reducers, is explained in Subsection 3.1. In SDWSN network, the total communication cost when the RVRR protocol is used is explained in subsection 3.2.

3.1 Routing Via Respective Reducer Protocol

This segment examines a method for steering bundles to the sink hub as effectively as conceivable to lessen the organization's all out correspondence costs. Conventional WSNs send data to the closest aggregator node or the sink node for aggregation. On the other hand, even in cases when reducers of different sensor kinds are in close proximity, the RVRR protocol passes the data to the relevant reducer in charge of the respective sensor type for aggregate.

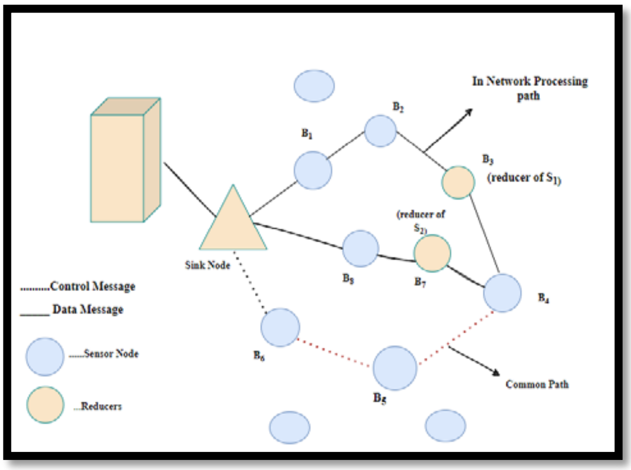
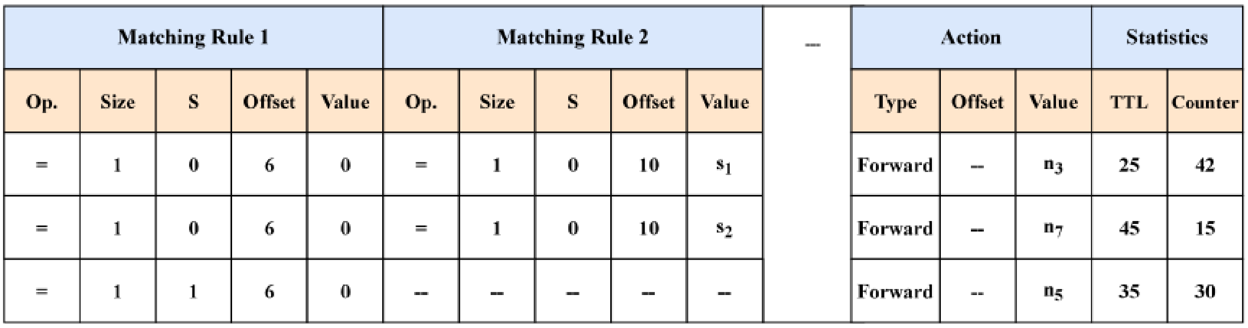


Figure 2: Example of routing in RVRR protocol

To limit the organization's absolute correspondence cost, the hubs should course their information parcels towards their distributed minimizer and their control bundles towards the sink hub by means of the briefest direct for the best in-network handling of the RVRR convention. Figure 2 represents how control bundles go over the familiar method for arriving at the sink hub, while information parcels are communicated to the minimizers by means of the in-network handling way. Subsequently, the organization in general takes advantage of the association and limit. All the more definitively, only one hub is picked as the minimizer for every sort of sensor Si. For instance, the minimizers for sensor types S1 and S2 are hubs N3 and N7, separately. Utilizing the stream table standards that the SDN regulator has set, different hubs in the organization present their <s,v> matches to the proper minimizers [14]. The information bundles of sensor type S2 that hub N5 created at time t in the model above should be sent to hub N7. Additionally, the parcel made by hub n4 at time t relates to s1 as far as sensor type; subsequently, it must be steered to hub n3, which is s1's comparing minimizer. While they don't yet yield information for a similar sensor type, any remaining hubs in the course go about as hand-off hubs by essentially sending parcels.



Matching Rule 1					Matching Rule 2					...	Action			Statistics	
Op.	Size	S	Offset	Value	Op.	Size	S	Offset	Value		Type	Offset	Value	TTL	Counter
=	1	0	6	0	=	1	0	10	s_1		Forward	--	n_3	25	42
=	1	0	6	0	=	1	0	10	s_2		Forward	--	n_7	45	15
=	1	1	6	0	--	--	--	--	--		Forward	--	n_5	35	30

Figure 3: Flow table of node n4

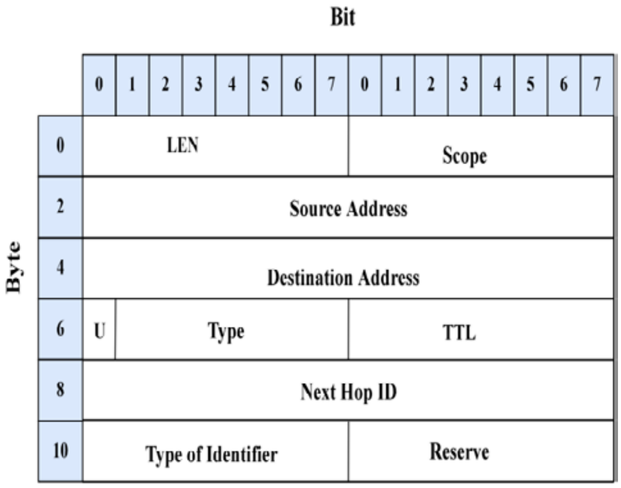


Figure 4: Packet header

Three of hub n4's entrances in the stream table are shown in the connected Figure 3. Parcels are steered as per the data gave in the stream table. The got parcel header fields are considered by the standards illustrated in the stream table. Figure 4 shows the parcel header utilized, which assists with explaining the sections in the stream table. The decent header of a RVRR bundle is comprised of 12 bytes. The last two bytes of the header are added to indicate the sensor type for which the hubs create bundles, while the initial 10 bytes of the header compare to the Child WISE parcel header. The main byte of the parcel header's stling of bytes is determined by the offset in the matching standard. The size of the field that should be parsed in the parcel header is demonstrated by size (in bytes). For example, in the primary passage, the bundle is sent to hub n3 in the event that it contains a worth of O (information parcel) in offset 6 and a worth of s1 in offset 10. Essentially, the third section should be directed to hub n5 on the grounds that it needs to follow the well-known way to arrive at the sink hub, and the worth in offset 6 is equivalent to 1 (i.e., the report parcel). Calculation 3.1 gives a definite clarification of the means engaged with the RVRR convention.

Following organization instatement, the hub's battery level and bounce count are communicated all through the organization as a feature of the Guide parcel, which contains these two snippets of data. At the point when the hubs get the Signal parcel, which is then shipped off the regulator, they record these subtleties in the neighbour list. Getting the geography perspective on the hidden organization is made conceivable by the geography information gathered from the sensor hubs. The data should be reliable on the grounds that WSN is an exceptionally powerful climate and the regulator relies upon information from sensor hubs [15]. Therefore, Signal bundles are steered temporarily. The undertaking that every sensor hub requirement to detect at time 'C' is allotted to it. Stages 8 through 19 of Calculation 3.1 are completed by the SDN regulator to pick the best minimizers for the organization. The regulator in a flash introduces F(R,j) into the minimizer hubs in the wake of choosing the minimizers. Let εj and εthr address the capacity limit and the minimizer hub's handling ability, individually.

Algorithm 3.1: RVRR routing algorithm:

Algorithm 3.1 RVRR routing algorithm:

```
1.  Begin
2.  Initialize the network
3.  Broadcast BEACON packets to the nodes
4.  Assign task $s_i \in S$ to all sensor nodes, such that no neighboring nodes execute the same task at time t
5.  $I^* n_s \subset N$ should run task $s_i$ at time slot $\tau^* /$
6.  Update flow table entries of sensor nodes
7.  while 1 do
8.  Initialize game $g = \left(N, (A)_{i \in N,} (u_i)_{i \in N}\right)$
9.  int timer = 0;
10. start the timer
11. for task s=1 to k do
12. for nodes n=1 to m do
13. max $\left(u_i(a_i(t), a_{-i}(t)\right)$
14. $I^* where\ u_i\ \left(a_i(t), a_{-i}(t)\right) = \beta^I \sum P_{ij} r_{js} \omega_j - cost_i * I$
15.  n++;
16. s++;
17. end for
18. end for
19. Reducer $n_j$ is chosen for each task $s_i \in S$
20. the reducer function F(RJ) is loaded on all reducers dynamically
21. Wait until an interrupt occur
22. if $u_j \le u_{thr} \| E_j \le E_{thr}$ then
23. Goto step 11
24. else if max (time) expires then
25. Goto step 11
26. else wait for mx (timer)
27. end if
28. end while
29. if sensor node then
30. wait until an interrupt occur
```

```
31. send REPORT packet for every time interval
32. generate data for assign task $s_i$ in time slot $\tau$
33. Receive packet:
34. if data packet then
35.     send to designated reducer via in-network processing path
36.     Wait for Max _t
37.     $I^*$until the reducer $n_j$ gets data from all nodes that execute task $s_i$ at time slot $\tau^*/$
38.     Execute reducer function F (R, $j$)
39.     send the resultant data packet to sink node
40. else if control packet then
41.     send via common path to sink node
42. else drop the packet
43. end if
44. end if
45. End
```

The regulator will start Stages 8 through 19 if either µ1 falls underneath the edge esteem or the minimizer's energy falls beneath the energy limit. In any case, before the regulator is utilized to play the following game, the minimizer hubs stand firm on their foothold for Max (clock).

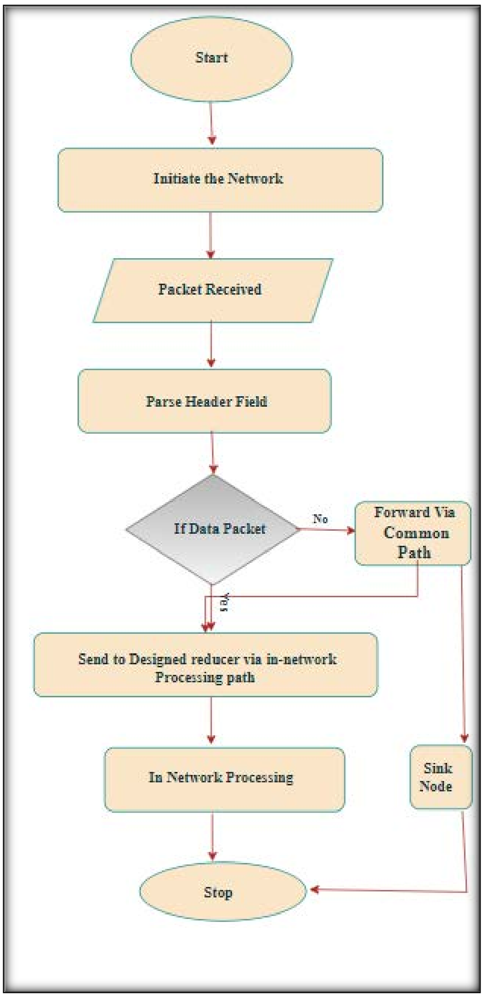


Figure 5: Process of routing in RVRR protocol

Although the sensor nodes are equipped with several sensors, they only produce traffic for a single kind of sensor in accordance with their assigned tasks. Stages 31 to 42 of Calculation 3.1 are directed by sensor hubs in the framework layer. The hubs glance through their stream table when they get a parcel and direct it to its planned objective. The bundle that the normal hub gets is either steered over the normal channel to the sink hub, which is the single correspondence connection point to the SDN regulator, assuming it is a control parcel or coordinated towards its comparing minimizer in the event that it is an information parcel. The minimizer plays out its minimizer capability in the wake of hanging tight for Maxt time. To decrease blockage and amplify channel limit, Maxt should be cautiously and carefully chose. Minimizers would start handling and conveying the subsequent information to the sink hub before it gets each of the information from the hubs if Maxt is excessively short, which would over-burden the divert and cause clog in the associations. In the event that the term is extremely extensive, the channel will remain inactive while sending information for a lot of time may be used. It is possible for the hubs to get parcels that were not implied for them since the channel is remote and has boisterous and loss correspondence associations.

In this scenario, the packet will be dropped by the nodes. Figure 5 depicts the whole RVRR protocol procedure.

3.2 Communication Cost of RVRR Protocol

The RVRR protocol aims to provide an efficient communication protocol for SDWSN networks by gradually reducing node energy usage. It is important to note that because communication-related activities need more energy than computation-related operations, the cost is defined in terms of these operations. Distance and traffic volume are the primary determinants of communication costs. The amount of data carried by the network is known as its traffic load, and it is directly impacted by its size. The number of nodes that send comparable types of data along the route, the packet arrival rate, and the packet size all affect the traffic load on a connection from ni to nJ. Presumably, the generation of type si packets follows the Poisson process with a rate of λsi. Let cli; be the capacity of link li and $\left|X_{n_i}^{(s_i)}(t)\right|$ be the number of data packets of type si transferred through the link li. ψi is a symbol for data packet size. The strain placed on sensor node ni by nodes producing values for comparable sensor types Si at moment t, $\widetilde{X}_{n_i}^{(s_i)}$ (t), is given in (1.2) as:

$$\widetilde{X}_{n_i}^{(s_i)}(t) = \frac{\Psi_i\left|X_{n_i}^{(s_i)}(t)\right|}{c_{l_i}};\ \forall\, n_i \in N, s_i \in S \qquad (1.2)$$

Let rjs be the binary variable that indicates if node nj is the matching reducer for task si, and let Pis be the probability that node ni is producing value for sensor type si. Dij is the hop-count between nodes ni and nj. Additionally, the controller, which is cognizant of the network architecture, computes the value of Dij. While $\widetilde{X}_{n_i}^{(s_i)}$ is its own information and is the information traffic load from sensor hubs ni. (1.3) gives the correspondence cost of moving information bundles from sensor hubs in the organization to the minimizers that are doled out to them:

$$\text{Cost}_{\,(i\leftrightarrow i)} = \sum_{i=1}^{m}\sum_{j=1}^{r}\sum_{s=1}^{k}\left(\widetilde{X}_{n_i}^{(s_i)}P_{is}r_{js}D_{ij} + \theta\right) \qquad (1.3)$$

The minimizers do their conglomeration capability, which is a typical capability in this work, in the wake of getting information from every sensor hub that delivered incentive for work Si, to which it is relegated as a minimizer. After the minimizer capability is executed, let Φj address the quantity of parcels moved from the minimizer hubs to the sink hub sn. The distance between the minimizer hub and the sink hub is indicated by D jsn. (1.4) gives the value paid to moving decreased parcels from minimizer hubs to the sink hub:

$$\text{Cost}_{\,(j\leftrightarrow sn)} = \sum_{j=1}^{r}\sum_{s=1}^{k}\phi_j r_{js} D_{jsn} \qquad (1.4)$$

The correspondence cost for moving information parcels from the sensor hubs to the minimizer and the correspondence cost for moving the produced information from the decrease hub to the sink hub amounts to the all-out correspondence cost in the organization. Thus, (1.5) gives the all-out cost (Cost generally) of sending the information parcels of each and every sort of sensor from sensor hubs across the organization as:

$$\text{cost}_{(\text{overall})} = \sum_{j=1}^{r}\sum_{s=1}^{k} r_{js}\left[\phi_j D_{jsn} + \sum_{i=1}^{m}\left(\widetilde{X}_{n_i}^{(s_i)}P_{is}D_{ij} + \theta\right)\right] \qquad (1.5)$$

The general expense of correspondence in the organization is the amount of the correspondence costs brought about when information bundles are sent from the sensor hubs to the minimizer and when delivered information is moved from the decrease hub to the sink hub. In this manner, the complete expense (Cost by and large) of sending information bundles of every sort of sensor from sensor hubs all through the organization is surrendered.

3.3. Performance Evaluation

The exhibition of the RVRR convention is surveyed as far as correspondence cost, energy utilization, network lifetime, and normal start to finish postpone utilizing the Organization Test system (NS-3). The RVRR convention is contrasted and three pattern conventions viz., (I) minimizer determination utilizing ILP technique - a SDN-based system that utilizes the most appropriate hubs as minimizers utilizing ILP, SDN-Savvy, a SDN based directing convention that conveys chain situated in-network handling and R-Drain, a customary steering convention for WSN which chooses CH in view of leftover energy to do in-organize handling.

3.3.1. Experimental Setup

In SDWSN setting, where programmable sensor nodes are transported in an ad hoc fashion throughout a 1000 m x 1000 m association area. The SDN-Canny show architecture and its bundle kinds are embraced by these sensor nodes. Every sensor node should communicate with the controller via the sink node as it is the designated point of interaction between the two. Because it is located outside the WSN, the controller is shielded from the destructive effects of power outages. At the start of the test, all of the sensor nodes communicate with the controller via Report bundle, providing details about their neighbours. This allows the controller to keep track of the area and the limits of each node. With this data, the controller may play the game in the control layer and choose the minimizers—one for each kind of sensor—as previously determined. At the point when the minimizers are selected, the essential standards are transmitted as a packet in message to get shown in the stream tables of all the sensor centres in the association.

The building strategy takes into account a central energy use radio model for sensor and sink centres in relation to route accidents. The very long distance between the sender and receiver determines the channel models. The open space (d2 influence mishap) or multipath obscuring (d4 impact setback) models are used if the distance (d) between the transmitter and the receiver (the centre of the transmitting and receiving, respectively) is less than the predetermined edge (dih). On the provided association district, there are m designated centre locations. On average, there are m/k nodes responsible for carrying out the job Si if there are k tasks. The energy required to transmit and receive signals, as well as store data, is dispersed by each minimizer.

The energy distribution is based on a free space power loss model as each normal hub should only forward data to its own minimizer. Compared to minimizer hubs, conventional hubs consume less energy. Keep in mind that at some point throughout the simulation, each hub in the organization would have the chance to assume the role of the minimizer hub. This ensures that the energy is consistently distributed throughout the entire organization. Table 1 provides a selection of the re-enactment borders that were used for this investigation.

Table 1: Simulation parameters of RVRR

PARAMETER	VALUE
Network dimension	1000 m x 1000 m
Number of nodes	250
Transmission range	100m
MAC protocol	IEEE 802.15.4
Size of data packet	127 Bytes
Initial energy	*SJ*
Edis	50 nJ/bit
Emp	0.0013 pJ/bit/m4
Efs	10 pJ/bit/m2
Data rate	250 kbps
Buffer size of sensor node	120 data packets
Simulation time	300 s

3.3.2 Performance Metrics

In order to validate the suggested framework, many execution metrics are taken into account, such as energy consumption, start-to-finish delay, communication cost, and network lifetime. Here we will take a quick look at the exhibition measures and see what they mean:

- **Communication cost:** The cost evaluation metrics are based on the evaluation in the relevant region. As a consequence of completing in-network dealing, the total correspondence cost for transporting data packages to the sink centre point is provided.

- **Network lifetime:** From the moment hub sending begins until the whole organization is deemed non-utilitarian, this is the time range in question. The organization's lifetime is the time it takes for the first hub to switch off for SDWSN monitoring applications that need intermittent data collecting.

- **Energy consumption in the network:** It is the aggregate sum of energy consumed by the hubs in the organization for parcel transmission, gathering, calculation, and inactive circumstances.

3.4 Novelty of the study

The RVRR (Resource-Aware Virtual Ring Routing) algorithm presents a novel approach to routing in sensor networks compared to traditional methods. It introduces several innovative elements, including dynamic task assignment, game-theoretic decision-making, adaptive resource management, and in-network data processing. By dynamically assigning tasks to sensor nodes and ensuring task diversity among neighboring nodes, the algorithm optimizes resource utilization and prevents conflicts, thus improving overall network efficiency. The incorporation of game theory enables nodes to make strategic decisions considering utility functions, costs, and rewards, leading to more efficient task execution. Additionally, the algorithm adapts its resource allocation based on factors such as utility thresholds and energy levels, enhancing its robustness in dynamic network environments. Moreover, by performing data processing and aggregation closer to the data source through in-network processing, the algorithm minimizes data transmission overhead and latency, improving overall network performance. This comprehensive approach to routing addresses key challenges in sensor networks, such as resource constraints and dynamic network conditions, making it a promising advancement in the field.

3.5 Contribution to the study

The integration of reducers within the infrastructure layer marks a significant departure from traditional routing paradigms in SDWSNs. Reducers, typically employed in data processing frameworks, are strategically positioned within the network to aggregate and process data closer to the source, minimizing energy-intensive communication overhead. In the context of routing protocols, the inclusion of reducers enables the offloading of computational tasks from resource-constrained sensor nodes, thereby reducing their energy consumption and extending their operational lifespan. By dynamically redistributing routing responsibilities to reducers, the proposed protocol achieves a more energy-efficient and scalable routing infrastructure compared to conventional approaches.

3.6 Utilization of the RVRR routing protocol

The RVRR routing protocol embodies innovation by employing a shortest-path selection strategy for forwarding control packets. Leveraging techniques from virtual ring routing, RVRR dynamically constructs and maintains routing paths that minimize latency and optimize resource utilization. By prioritizing the shortest path for control packet transmission, the protocol enhances network responsiveness and reliability, crucial for real-time communication in smart environments. This approach not only reduces packet delivery latency but also conserves energy by minimizing the distance traveled by control messages. Thus, the innovative application of RVRR in the proposed concept demonstrates a significant advancement in routing efficiency and reliability within SDWSNs.

4. Results and Analysis

The correspondence cost experienced by the organization concerning the hub include is displayed in Figure 6. The outcome is gotten for a shifting number of minimizers. It is seen from the diagram that the expense increments as the hub's include in the organization increments. Correspondence cost caused by hubs is reduced when the number of minimizers is greater [16]. This is because hub degree is an option standard in the game shown in RVRR. Consequently, hubs that are associated with a more noteworthy number of hubs detecting comparable occasions are chosen as minimizers. It should also be noted that the cost is dependent on the volume of traffic and the distance between the hubs. Having many minimizers allows an organization to significantly cut the cost of transmitting packages to each one.

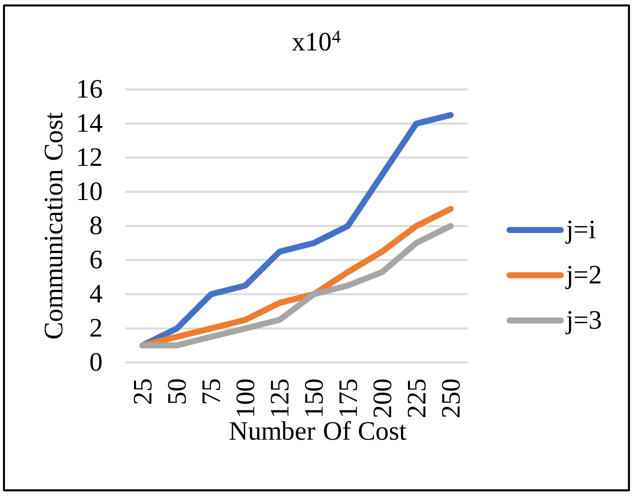


Figure 6: Communication cost with respect to number of nodes for varying number of reducers (j)

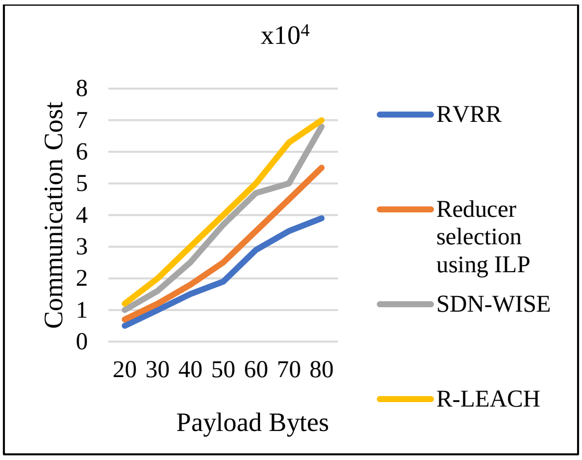


Figure 7: Communication cost with respect to payload

Likewise, Figure 7 displays the communication cost of the organization about the payload. Using RVRR protocol, 200 transmitted sensor hubs with r = 3 and k = 3 are used to construct the output. The graphic clearly shows that the communication cost of the RVRR convention is cheaper than other conventions at different periods, as the cost of transferring the resultant packages from minimizers to the sink hub is not essential. The value of cpj is 1, and the values of Dij and D jsn will always be zero since the SDN regulator chooses the minimizer in a certain way. Compared to minimizer choice using the ILP approach, SDN-Shrewd, and R-Filter, RVRR outperforms them all in terms of correspondence cost by 22.72%, 43.46%, and 49.04%, respectively.

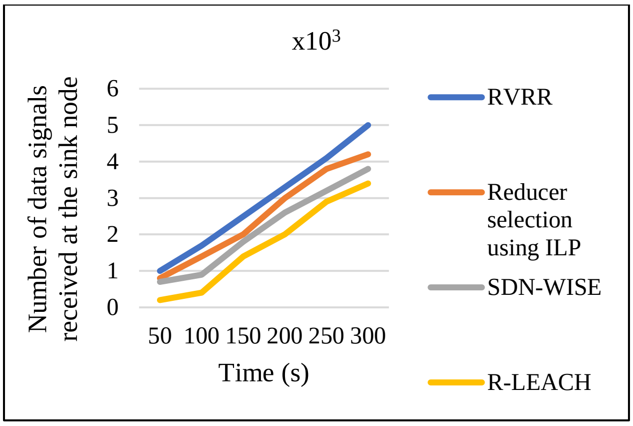


Figure 8: Numbers Of Data Signals That the Sink Node Received Throughout the Experiment

The quantity of information signals received at the sink hub throughout the re-enactment is seen in Figure 8. A key idea in sensor organizations is quality. The kind of problem depends on who gets more ward information: the end client or the washbasin hub. When hubs do not recognize similar events, it is crucial to provide the sink hub enough information to avert application-related catastrophes in a multitasking context. The findings indicate that RVRR sends more data in comparison to other conventions. The rationale is that RVRR requires much less time to choose the minimizer and carry out the minimizer functions than other existing conventions. Information bundles also have reduced latency in reaching their destination, as shown. Even if the amount of data received at the sink hub in the allocated time is less than RVRR, there is still a discernible delay when determining the minimizer using the ILP technique. Because of SDN-Astute and R-Drain, there will be a significant bundle loss rate owing to blocking, which will result in lost packets being retransmitted repeatedly. As a result, the data sets will be unable to arrive at their intended location on time.

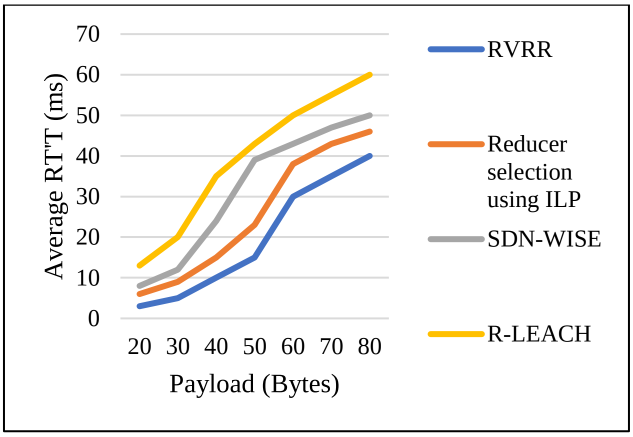


Figure 9: Impact of payload on RTT

Figure 9 shows an RTT correlation for different payload sizes. RTT is the amount of time it takes a hub to estimate how long it will take to transmit a bundle and get shipping confirmation. It is found that a number of parameters, including the number of hubs, distance, payloads, clog, hub handling capabilities, regulator reaction time, and blockage, affect RTT. The findings demonstrate that as payload grows, RTT rises gradually. However, RVRR packages have a lower RTT than other conventions. This is as a result of the RVRR convention bundles having shorter latency, as shown. Similar to information packets, request packets are not required to use the same route; instead, they might choose the shortest path possible to reach their destination, which reduces channel congestion [17]. In contrast, the CH is in charge of sending control and data packets to the sink hub when using R-Drain. The traffic burden of the organization is increased by all of this. While the ILP technique and SDN-Attune setting have reduced the amount of control messages in the minimizer option, no specialized model exists for load adjustment or reducing blockage. Thus, as compared to minimizer choice using the ILP technique, RVRR lowers RTT by 29.28%, while SDN-Savvy and R-Drain reduce RTT by 43.81% and 57.22%, respectively.

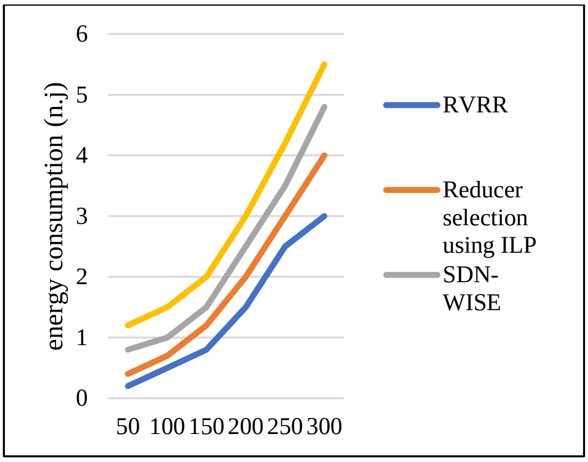


Figure 10: Average energy consumption with respect to time

Essentially, the typical energy utilization in the organization for reproduction time and the payload is displayed in Figure 10 and Figure 11 separately. Because a big message means a long radio transmission and a high live time, which suggests that hubs use more energy, payload has a basic impact on how much energy hubs use.

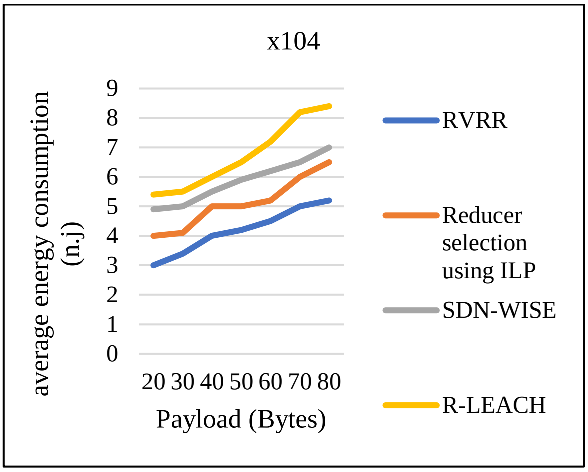


Figure 11: Effect of payload on energy consumption

The amount of data that needs to be sent directly affects the amount of energy that the hubs are expecting, denoted as b. The results show that, as the payload increased, so did the energy consumption. No matter the amount of the payload, RVRR consistently outperforms other conventions across varying time intervals. Since the game model uses the hub degree as a determinant to assign the hub as a minimizer, the hub with the highest hub degree is picked as the minimizer. This leads to the inference that. Therefore, it is not necessary to send the packages across a great distance before they are tallied. With varying payload sizes, RVRR demonstrates an 18.80% reduction in energy consumption compared to minimizer choice

using the ILP approach, a 28.65% reduction compared to SDN-Astute, and a 37% reduction compared to R-Drain.
Figure 12 demonstrates the organization lifespan of RVRR, SDN-Astute, minimizer determination using ILP, and R-Drain conventions about the number of hubs. The lifespan of the framework is seen to be greater for small organizations and to continually decrease with larger organizations. The hubs will continue to serve their purpose for a longer duration as a result of the uniform energy dispersing over the RVRR organization area.

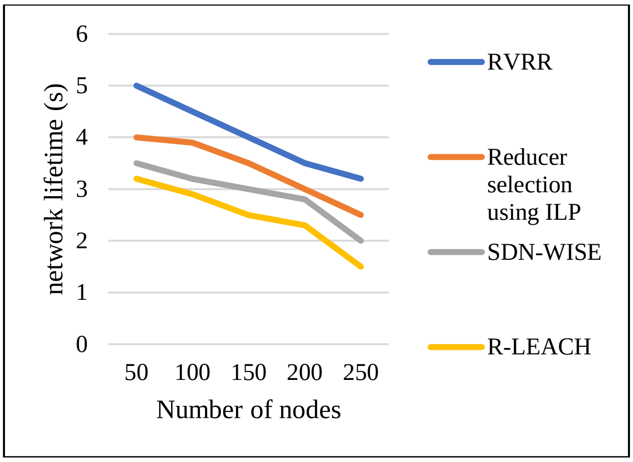


Figure 12: Comparison of network lifetime

Furthermore, the SDN controller runs some of the power-hungry features, such as game model execution and appropriate minimizer determination. The sensor hubs' energy consumption is greatly reduced as a result. The hubs channel their energy quicker than in RVRR because even with the CH pivot activated in R-Filter, a lot of control messages (Ad, Join-Solicitation, to name a few examples) still need to be transmitted across the organization. When everything is said and done, the RVRR convention extends the life of the organization by 19.45% when compared to minimizer determination using the ILP technique, 39.16% when compared to SDN-Astute, and 54.60% when compared to R-Drain.
As shown in Figure 13, the hubs often wait for a variety of payloads to change before moving on. Delay is a major problem in simple WSN applications. Insignificant postponement is accomplished just when the heap is even across the whole organization. The outcome shows that the parcels of RVRR experience less postponement than different conventions.

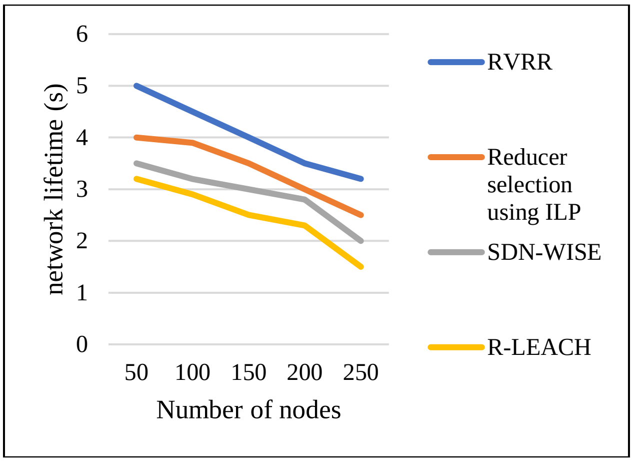


Figure 13: Payload's effect on the total delay

This is on the grounds that RVRR utilizes two ways, in particular the in-network handling way for information bundles, and the familiar way for control parcels. In this manner, the parcels need not sit tight in the information line for a more drawn-out time frame. Besides, the utilization of various ways for control and information bundles assists with guaranteeing appropriate channel use. This fills in as an additional justification for information bundles to arrive at the objective quicker. Reasonable minimizers and the view update both take non-trivial amounts of time due to minimizer determination using the ILP approach. Definitively, in a powerful evolving climate, the intricacy is reasonable, and delay is huge. Consequently, RVRR diminishes the start to finish postpone by 11.70% over minimizer choice utilizing the ILP strategy, 18.53% more than SDN-Insightful, and 23.96% over R-Filter.

4.1 Limitations of the Study

While the study presents promising results regarding the benefits of the RVRR protocol in IoT applications within smart environments, it's essential to acknowledge several limitations:

1. The study might have focused on a specific set of IoT protocols and environments. Therefore, the findings may not be generalizable to all IoT scenarios. Different environments, network setups, and application requirements could yield different results.
2. The study likely utilized simulations to evaluate the performance of the protocols. While simulations can provide valuable insights, they may not fully capture real-world complexities and nuances. Factors such as hardware limitations, network congestion, and

environmental interference may affect protocol performance differently in practice.

3. The study may have relied on certain assumptions and parameters in the simulation setup, which could impact the validity of the results. For instance, network traffic patterns, node mobility, and energy consumption models used in the simulation may not accurately reflect real-world scenarios.
4. The study might not have considered the practical challenges associated with implementing the RVRR protocol in real IoT systems. Factors such as protocol overhead, compatibility with existing infrastructure, and ease of deployment could affect its feasibility and adoption in actual deployments.
5. While the study evaluates the performance of the protools based on metrics such as communication costs, energy consumption, and network lifespan, other relevant metrics such as scalability, reliability, and security might not have been thoroughly examined.

5. Summary

This paper presents RVRR convention, an energy proficient directing convention for SDWSN that acts in-network handling to altogether decrease the organization's general correspondence cost. Consequently, a revised game model is implemented to iteratively choose the appropriate hub to serve as the minimizer, responsible for carrying out the minimizer function and transmitting the resulting data to the sink hub. Besides, by coordinating information and control bundles in various ways, network idleness is altogether diminished. The trial results uncovered that RVRR performs well in the SDWSN climate as far as correspondence cost, energy circulation, and deferrals. Definitively, the nature of detecting is ensured by the exchange of adequate information to the sink, in this manner helping the application clients. However, RVRR strikingly lessens the information parcels in the organization, the trading of control bundles to get an exhaustive perspective on the geography is high.

References

[1] Amadeo, M., Campolo, M., & Molinaro, A., A survey on the use of wireless sensor networks for industrial applications. IEEE Sensors Journal, 2020, 20(10), 5818-5839.

[2] Balasubramanian, S., & Sivakumar, D. , A survey on IoT protocol stack for smart cities. In Proceedings of the International Conference on Electrical, Electronics, and Computer Science (ICEEECS),2019, 1-8.

[3] Mahmood S. Mahmood, Najla B. AI-Dabagh, Improving IoT Security using Lightweight Based Deep Learning Protection Model, Tikrit Journal of Engineering Sciences, 2023, 30 (1), 119-129.

[4] Boualem, M., & Bhuiyan, M. A. A. , A survey on industrial IoT security with blockchain technology. IEEE Consumer Electronics Magazine,2019, 8(4), 62-70.

[5] MahbubaAfrin1, & Redowan Mahmud, Software Defined Network-based Scalable ResourceDiscovery for Internet of Things, EAI Endorsed Transactions on Scalable Information Systems, 2017, Volume4, Issue14.

[6] NarayanDG, RashmiB., PavitraH, YashawardanD, AframeworkforDataProvenanceAssuranceinCloudEnvironmentusingEthereumBlockchain, EAI Endorsed Transactions on Scalable Information Systems, 2024, Volume 11, Issue 2.

[7] Chen, M., & Hu, Y. C. , A survey of LPWAN technology for IoT-based smart cities. IEEE Access, 2018, 6, 7616-7632.

[8] Cui, Y., Zhang, Y., Zhao, Y., & Li, Y.,A survey of network protocols for low-power wide-area networks in smart cities. Sensors, 2019, 19(1), 114.

[9] Shen, Y., Zhang, T., Wang, Y., Wang, H., & Jiang, X. (2017). Microthings: A generic iot architecture for flexible data aggregation and scalable service cooperation. *IEEE Communications Magazine*, *55*(9), 86-93.

[10] Zhang, Y., Shen, Y., Wang, H., Yong, J., & Jiang, X. (2015). On secure wireless communications for IoT under eavesdropper collusion. *IEEE Transactions on Automation Science and Engineering*, *13*(3), 1281-1293.

[11] Wang, H., Zhang, Z., & Taleb, T. (2018). Special issue on security and privacy of IoT. *World Wide Web*, *21*, 1-6.

[12] Lakshmi, M. S., Kashyap, K. J., Khan, S. M. F., Reddy, N. J. S. V., & Achari, V. B. K. (2023). Whale Optimization based Deep Residual Learning Network for Early Rice Disease Prediction in IoT. *EAI Endorsed Transactions on Scalable Information Systems*, *10*(6).

[13] Zhu, X., Hu, C., Lu, Y., Wang, Z., & Xue, H. (2023). Lightweight Cryptographic Simulation of Power IoT Fused with Bayesian Network Algorithms. *EAI Endorsed Transactions on Scalable Information Systems*, *10*(4), e1-e1.

[14] Li, S., Xu, L., & Zhao, S., 5G Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 2018, 20(3), 2244-2253.

[15] Mahmood, A., Ullah, F., & Shah, G., A survey of security challenges in smart cities. IEEE Communications Surveys & Tutorials, 2020, 22(2), 733-764.

[16] Mtibaa, A., & Mahmoudi, H., A survey on machine learning for predictive maintenance in the IoT context. IEEE Access, 2019, 7, 16283-16303.

[17] Raza, A., Kulkarni, P., & Somayaji, M. K. , Low-power wide-area networks (LPWANs): Towards sustainable IoT applications. IEEE Communications Magazine, 2019, 57(5), 70-77.

[18] Kanellopoulos, Dimitris, et al. “Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives.” *Electronics*, vol. 12, no. 11, 31 May 2023, pp. 2490–2490, https://doi.org/10.3390/electronics12112490.