Journal of Information Systems Engineering and Management
2025, 10(19s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

Efficient Routing for Internet of things to Reduce Energy Consumption in the Network

Priya Ranjan Raj[1] Raman Kumar Mandal [2] Shiva Kumar[3] Shaffy Bains [4] Abshiek Jha [5] B.Jyothna [6]

1priyaranjanraj6153@gmail.com2 reffect1985@gmail.com 3 drshivakumar1978@gmail.com 4 shaffy18@gmail.com 5 abhijihal495@gmail.com 6 Jyothsnab.cs@gmail.com

ARTICLE INFO

Received: 19 Dec 2024

Revised: 29 Jan 2025

Accepted: 12 Feb 2025

ABSTRACT

In this study, we propose an optimization method for transportation problems utilizing Generalized Intuitionistic Trapezoidal Fuzzy Numbers (GITFNs). This method effectively handles uncertainty and imprecision in transportation systems, enabling more realistic and reliable decision-making. A GITFN-based transportation model is developed, incorporating fuzzy costs, capacities, and demands. An optimization algorithm is designed to minimize transportation costs while satisfying supply and demand constraints. The method is applied to a numerical example, demonstrating its efficiency in solving complex transportation problems. The results show significant improvements in transportation effectiveness and cost reduction.

Keywords: IoT, Clustering, Cluster Head, VGDRA

I.INTRODUCTION

With technology growing faster and digital assistants being used more in all aspects of life and work, further development in these areas must be done. A key concept enabling this progression is the IoT, which connects devices entrenched within various objects. Routing protocols must be developed to support communication in a decentralized, self-organized, and dynamic infrastructure to realize IoT. IoT envisions machine-to-machine communication between devices, referred to as smart objects [1]. In comparison to classical Wireless Sensor Networks (WSNs), IoT devices are quite compact, embedded systems that are constrained in their resources, an average of a few hundred kB of ROM, and operated by batteries that are designed to last for several years or months without service. These devices construct a mesh system and access the cyberspace via a gateway router. On the Internet, IoT traffic is typically low-volume, bursty, and consists of small payloads with no connection. The usage of traffic patterns is application-based. Building Automation usually consists of point-to-point traffic, whereas in home Automation applications often there is a amalgamation of multipoint-to-point and point-to-multipoint communication [2]. Wireless mesh networks can face serious problems like signal interference, fading connectivity, and reflection or scattering which are the reasons why reliable bidirectional communication is not always guaranteed in this case.

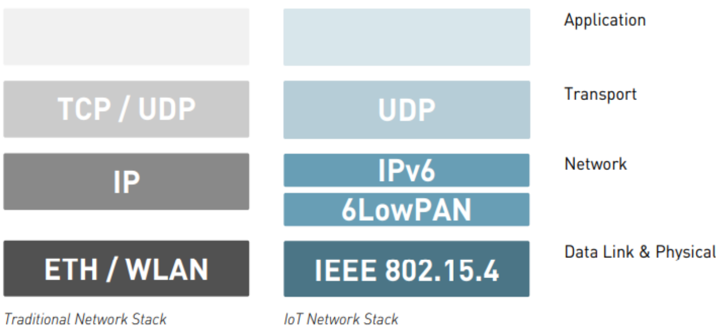

Figure 1: Comparing Conventional and IoT Network Stacks.

The IoT being so diverse from the Internet is the basic reason to differentiate between them and thus a special network stack represented in figure 1 is essential. The IEEE 802.15.4 Data Link and Physical layers are designed for power-saving applications and low-cost devices. They come with a MTU (Maximum Transmission Unit) of just 127 bytes. This contradicts the requirement of the IPv6 minimum MTU (1280 bytes) [3]. Hence, it is a necessity to use adaptation layer 6LoWPAN. Over there, IPv6 headers are condensed and those packets that are more than the 127-byte MTU are fragmented. The border routers, which are the devices that connect the 6LoWPAN network with the larger Internet, are capable of reassembling these fragments

A. Requirements and key challenges for routing protocols

Routing protocols have various requirements tailored to specific IoT scenarios, such as smart home systems, urban LLNs (low-power and lossy networks), and building computerization. In spite of these fields being IoT-related, they vary greatly in traffic flow, network size, and mobility. The requirements for routing protocols, even so, can be summarized into following groups:

1) ***Traffic Patterns:*** A routing protocol should match the distinct traffic patterns of a given application field. While traffic patterns shift from one network to another, a single protocol can hardly fit all IoT applications. On the contrary, specialized protocols have to be designed for different IoT subdivisions.

2) ***Energy efficiency****:* A key concern in the IoT is energy-saving as a lot of the devices work on batteries and need to be operated for a long time. Thus, the acquisition of such routing-based mechanisms that are energy-efficient and capable of managing node's energy constraints to find an optimal route is necessary [5].

3) ***Scalability:*** The protocol should be able to function well at different scales of the network including one with a size of just 100 to a very large one with 1,000,000 nodes and the efficiency should remain unaffected both in terms of memory usage and routing table size while the network becomes larger.

4) ***Mobility****:* Despite the fact that IoT networks are mainly static, a good routing protocol should be able to adapt to occasional mobility of the nodes.

5) ***Bidirectionality:*** Bidirectionality is the key since wireless networks are not always guaranteed to have bidirectional connectivity. Routing protocols should avoid and detect unidirectional links if possible, and otherwise, utilize them effectively in a single direction

6) ***Transmitter usage:*** Power usage associated with the transmitter is the primary cost for constrained devices. Therefore, it is advisable to use it as sparingly as possible.

B. Protocol characteristics

All routing protocols consist of core basic principles that are the bases for their working. This section will discuss the characteristics that are probably the most beneficial in an IoT context.

1) ***Proactive vs. Reactive:*** Besides hybrid methods, routing protocols are categorized into proactive and reactive ones. Proactive protocols collect routing information constantly to have an accurate view of the network topology [7]. Nodes use periodic beacon transmissions to check their connections with their neighbours. Thus, they have a low latency but consume more battery life. This is because most of the exchanged topology data is unnecessary overhead in networks with infrequent traffic, which leads to the depletion of devices' batteries. Different from the proactive protocols, reactive protocols only look for the routes when they are required. The procedure for discovering route is triggered by the start of a transmission to another node; therefore, the topology information is exchanged only when necessary and this way, saving energy. Nevertheless, this method results in higher latency, as routes are found on-demand, which leads to delays for the ones that are unknown or expired [8]. This is the case with the application or the protocol that must deal with the situation by temporarily storing or discarding data.

2) ***Hop-by-Hop vs. Source Routing:*** Both hop-by-hop and source routing can be used for packet forwarding. In hop-by-hop forwarding, each router holds only very little information about the route it participates in which is very important for the transmission of packets to the destination, namely the destination and the subsequent hop. In source routing, the whole route is included in the packet header. Although source routing is memory-efficient, it brings about a significant increase in header dimensions and traffic levels. Also, the routes may get outdated before the packet arrives. The challenge is even bigger in IoT environments with low MTU sizes, such as IEEE 802.15.4, and moderate node mobility [9].

3) ***Information Centric:*** The ICN (Information-Centric Networks) is a new paradigm in networking as it is not merely a routing protocol. The main idea of ICNs is to issue a request for data instead of asking for its source. Data is requested by nodes in the network rather than specific addresses. This type of service is suitable for some of them IoT use cases like environmental data collection, where the importance is on the information itself ICN can be one of the suitable IoT applications. Nevertheless, ICN was originally intended for large-scale, wired networks and presents difficulties for IoT deployments. For example, ICNs have a bidirectional connection without verifying this, which can be problematic in the IoT environment. Moreover, some of the ICN protocols require the [10] routers to cache the forwarded data, which in turn can be a problem since the memory of the IoT devices is limited. Yet another complication is that information is now mostly stored as new copies along with the regular updates instead of replacing the previous versions, thereby resulting in even more storage requirements

4) ***Multipath routing:*** A protocol using multipath routing looks for and utilizes alternative routes to reach the nearest destination. This way, the forwarding of packets is shared among more nodes, resulting in the conservation of energy of individual, heavily-used nodes.

5) ***Probabilistic routing:*** Routing with the help of probabilistic methods, involves the computation of routing decisions using probabilistic values. Gossiping is the easiest way to do it [11]. Here, a piece of data is propagated through the network like a rumor, with each packet being forwarded with a probability p. As a result, this method mitigates traffic overhead. An advanced technique is to follow the delivery tracker's location of the mobile node or recall the delivery history of the mobile node, estimate the delivery probability of the message to the desired destination, and make forwarding decisions accordingly.

C. Routing protocols

Following is the list of some common protocols for IoT.

1) ***RPL:*** RPL was more known for its application as a routing protocol for LLNs and the IoT. The main objective was to handle traffic in multipoint-to-point format predominantly. However, it can also support point-to-multipoint and point-to-point traffic to a limited extent. RPL presupposes that there is at least one sink node capable of processing data more intensively and containing more energy than the remaining ones [12]. Thus, the creation of a DODAG based on the sink node as the root node, consequently directing traffic towards it, is a solution for this problem. Every single node in the DODAG delivers DIO (DODAG Information Object) packets that contain the details of its identification and rank within the DODAG. It is thus possible to say that RPL is a proactive protocol because DIO messages are communicated proactively and the network topology is first explored. Nevertheless, the DIO transmission rate is reduced over time in order to save on unnecessary control overhead when the DODAG is stable. DAO (Destination Advertisement Object) messages that are enabled allow RPL to perform the detection of bidirectional connectivity, as well as the support multipath transmission from the sink node to the distinct routers, even though this increases control traffic and memory use [13]. Moreover, RPL is able to utilize source routing when it is in non-storing mode, thus making the protocol different from the other protocols discussed.

2) ***OLSR and OLSRv2:*** OLSR (Optimized Link-State Routing) and its successor OLSRv2 are proactive link-state hop-by-hop routing protocols as defined by IETF which are widely adopted among MANETs. One of the key improvements of OLSRv2 is its support for alternative metrics, for example, energy-aware metrics. OLSRv2 also supports extensions for multipath routing, which had already been detailed for OLSR. Nevertheless, both protocols are probably unsuitable for IoT environments. Being proactive, they can periodically send notifications to discover neighbours and control the topology. This results in broadcasting consumptions of unnecessary transmissions and battery [14]. Besides, they have all the information needed to know direct neighbours and routes all over the network, that is producing storage overhead due to keeping data that possibly will not be used in the Information Base.

3) ***Ad-hoc On-Demand Distance Vector (AODV):*** This protocol initiates a loop-free path on demand only when it is demanded. A mobile node can create and maintain a route only to the other node if it needs to deliever a message. Although the procedure of discovering route generates multiple routes, AODV chooses the best one and discards the others. Nevertheless, often occurring route breaks cause the intermediate nodes to drop the packets since no other routes are available, which in turn [15], diminishes the total throughput and the PDR. In the case of highspeed motion, the end-to-end delay might be extended due to continuous route discoveries. A route failure entails the route discovery process to restart from the beginning, thus making it more resource-consuming and increasing the overhead.

4) ***PRoPHET:*** The PRoPHET technology illustrates the impact of human movement and data traffic patterns in a network's environment. Delivery predictability is a indicator that shows the probability of data being effectively transmitted to each neighbour according to PRoPHET, thus, it is categorized as a probabilistic protocol. Data meant specifically for a specific route is temporarily held until a connection can be made, thus allowing PRoPHET to control the networks which are not completely connected all the time [16]. Two nodes in a network can be connected if they move in close proximity or if one turns on. The nodes transfer their calculated predictability information to each other and subsequently update their internal data. With the aid of this exchanged information, each node can analyse whether it wants to transmit any data to the neighbour it recently came into contact with. Along with that, a node can also direct its information through various other neighbours, thus, PRoPHET is a multipath routing protocol too.

II. LITERATURE REVIEW

A. S. Hampiholi, et al. (2018) presented an advanced GA (Genetic Algorithm) named MEGA, that combined a Local Search process and a Sleep-Wake Up process [17]. This method optimized WSN (Wireless Sensor Network) by dynamically saving energy and extending network lifetime while accounting for communication constraints and exhausted energy during sensor procedure. They compared the effectiveness of this MEGA protocol with routing methods to evaluated its capability with respect to routing effectiveness and exhausted energy. Software-based tools for simulation will be used for developing and performing the investigation of ad-hoc networking protocols. The operation of the system will be evaluated under various WSN situations and scenarios to demonstrate the increase in energy conservation and routing efficacy.

D. Airehrour, et al. (2019) introduced SecTrust-RPL to improve the standard RPL protocol by integrating a SecTrust (Secure Trust) system [18]. This protocol aimed to protect against different incidents by employing a trust-reliant process that detects and isolates these threats while also improving overall network effectiveness. Comparative analyses showed that SecTrust-RPL surpasses the typical RPL with respect to detecting and removing intrusions. This protocol's effectiveness and resilience have been validated through extensive simulations and testbed experiments. Ultimately, SecTrust-RPL showed the potential by means of trust as a robust safety framework to alleviate occurrences.

F. Al-Turjman, et al. (2019) suggested a technique for data distribution in extensive networks devoted to catastrophe management, making use of a huge number of sensing devices dispersed throughout metropolitan infrastructures, including parking lots at shopping centers, traffic systems, and airport facilities [19]. Information can be sent via relays from numerous sensor nodes to a gateway that is connected to a larger network, such as the Internet, thanks to this framework, which was created for energy-efficient Internet of Things applications. When choosing the next hop for routed packets in the WSN, this system considers the total network energy in addition to resource constraints like hop count and remaining energy levels. Extensive simulations demonstrated the effectiveness of the suggested approach in comparison to the literature's current energy-aware routing paradigm.

M. Conti, et al. (2020) employed SARP, a novel assessment-assisted safe and scalable routing protocol for Internet of Things networks, which carried out extensive attestation using the RPL technique [20]. This system not only improved network security against internal attacks but also protects RPL's data communication process, thereby improved overall network performance. SARP was designed to support network mobility, device heterogeneity, and scalability without compromising crucial IoT requirements like little overhead related to networks and low storage and energy use. Even with multiple kinds of attacks, SARP's effectiveness was demonstrated by simulation findings over a wide range of IoT scenarios in the light of several efficacy indicators.

N. Djedjig, et al. (2020) introduced MRTS provided a trust evaluation mechanism for stable routing topology construction [21]. This experiment showed that MRTS was efficient in many important areas, including packet delivery ratio, exhausted energy, changes in nodes' ranks, and overall throughput. Furthermore, mathematical model showed that MRTS satisfies essential criteria including consistency, optimality, and no loop. The trust-based routing metric that has been provided demonstrates repetitiveness and isotone, both of which are critical for routing protocols. In order to provide strategy in the iterated Prisoner's Dilemma, MRTS was developed using concepts from game theory, emphasizing its capacity to improve node cooperation. Results from evolutionary simulations and mathematical analysis both attest to the fact that MRTS successfully promotes stability and IOT evolution.

A.Kumar Dutta, et al. (2022) designed EMO-QoSCMR protocol for IoT-enabled WSN to optimized the QoS (quality of service) parameters, including energy efficiency, throughput, delay, and network lifetime [22]. This protocol operated in two stages: clustering and routing. At first, it used a CEROAC method to find an optimum suite of CHs and create clusters. Then, it used an OCGOR method to construct the best routing paths in the network. A fitness function was derived from main parameters like residual energy and closeness between two end points. The EMO-QoSCMR protocol showed a significant improvement, achieving a network active node (NAN) count of 64, in contrast to lower NANs of 2, 10, 42, and 51 rounds achieved by other versions (LEACH, PSO-ECHS, E-OEERP, and iCSHS respectively). The protocol's performance was evaluated in terms of energy conservation and network lifetime.

M. Shafiq, et al. (2021) designed RCBRP to define energy-efficient routing paths, thereby improving network lifespan [23]. This protocol was divided into six stages to facilitate the process and communication. They presented two primary techniques: the distance and depleted energy assessment methodology and the resource-efficient grouping and routing approach. By clustering smart devices, this scheme minimizes energy consumption and balances the load. Extensive simulations conducted using Matlab validate this method, demonstrating its superiority over existing methods in terms of exhausted energy, the number of packets received at the base station, and the number of active versus dead nodes. In further work, they plan to explored edge computing to further verify the effectiveness of robust clustering.

S. Sennan, et al. (2022) presented EACR-LEACH protocol for WSN in IoT applications. The main aspect of this clustering protocol is the selection of CH (Cluster Heads) [24]. In EACR-LEACH, CHs are chosen based on several routing metrics: RER, NoN, Distance to the Sink, and the NTNACH. Extensive simulations were performed using MATLAB 2019a, and the performance of EACR-LEACH was compared to the traditional LEACH and SE-LEACH protocols. The results showed that EACR-LEACH could extend the network's lifetime by 4% to 8% and improve throughput by 16% to 24%.

Naveen Kumar Gupta, et al. (2023) presented new AVDR protocol treats anchor nodes as sub-destinations, facilitating a more direct path between source and gateway nodes [25]. This system effectively bypasses void boundaries, allowing for direct connections between the source and anchor, from anchor to end point, or between consecutive anchors. Furthermore, anchor data is disseminated to the relevant areas, minimizing the need for periodic anchor advertisements. Testing conducted using genuine and OMNET++ simulator demonstrated that the AVDR protocol averages a data transfer time of just 29.09 ms. Furthermore, AVDR showed improvements in routing stretch of 8.2%, 7.54%, 7.66%, 8.49%, and 8.22% over these methods. It also significantly minimized network overhead, achieving improvements of 30.25%, 57.45%, 51.05%, 75.56%, and 58.89% compared to the aforementioned protocols.

H. Gul, et al. (2024) introduced the concept of traffic-aware, cluster-based, and power-aware routing approach aimed to optimized data delivery in networks by using traffic-aware and cluster-based strategies [26]. This protocol segments the network into clusters, selecting optimal cluster heads from both best and normal nodes based on their residual energy levels. It evaluated multiple criteria of performance. The protocol's performance was assessed using the NS3.40 network simulator. Results showed that across many traffic rates, node counts, and packet sizes, the presented approach surpassed LoRaWAN with regard to several performance indicators. Furthermore, this method demonstrated a 13% improvement in packet delivery ratio, a 10 ms decrease in latency, and a 10 mJ decrease in average spent energy when compared to LoRaWAN with 100 nodes.

III. RESEARCH METHODOLOGY

Data is gathered from specific cache nodes and sent to the sink via the proposed method, which relies on making a choice for cluster head (CH).

Data is gathered from specific cache nodes and sent to the sink via the proposed method, which relies on making a choice for cluster head (CH).

A. *Step 1: Cluster Head Selection*

The key objective of the clustered WSN application is to distributes nodes randomly. This methodology gives rise to the creation of CHs, which is, on the other hand, an arrival of some problems. One of the most considerable problems is the increased energy consumption of nodes, which means the careful management of CHs is needed to avoid disposability. In addition, reducing long-distance communication between CHs and placing motes nearer to them are important issues. The CH is the one that refers to the nodes that are below the expected standards which in turn is the cause of operational problems. These kinds of nodes experience difficulties in remote areas, thus, efficiency falls. The choice of such motes as CHs is dictated by the surge of intra-cluster energy, while on the other hand, the genuine motes, which just send and receive data, consume less energy overall. The system guarantees synchronization along a broad range of frequencies, which in turn, decreases the motes' battery consumption. While picking the paternal mote for the CHs, movements are optimized to ensure the maximum efficiency. Every sensing node (SN) gets better and better through a two-value function which helps picking the CH. The functions are made as per the node's degree, and the average power of the other motes is used to find the proximity of nodes to the sink. Motivated by full CH formation, the system produces lots of motes in a hurry. More CHs spread out along motes to minimize expensive communications. It consequently prolongs the network's lifespan by decreasing energy consumption. Let the process start with Hello message broadcasting. The second phase is to calculate the distance between all nodes and the sink. The following phase sends the INITIAL-MSG, which contains the identification and proximity between each mote and the sink, throughout the whole network. The key function is to determine the gap between a node and its adjacent ones, and the CH is found using the next computation method which is expressed by equation (1).

$$R_{CH} = R_{min} * [1 + (\frac{d_{BS} - d_{BSmin}}{d_{BSmax} - d_{BSmin}})] \quad (1)$$

This equation illustrates the smallest cluster size with R_{min}, acting as a protocol metric, where d_{BSmin} and d_{BSmax} respectively depict the distance of the closest the most distant nodes from the sink. Each mote is evaluated based on the value function, which determines its suitability for selection as a CH.

B. ***Step 2:Selecting Cache Node***

Energy clusters facilitate intra-cluster communication by supporting efficient components such as clusters. However, the process of a node utilizing energy and establishing communication within a cluster is resource-intensive, leading to an increase in intra-cluster energy consumption. This essay focuses on centrality. To lower the energy used for intra-cluster activities, the subsequent power average declines as the remoteness between the main cluster and the receiving node decreases. Several factors negatively affect energy consumption. Under challenging conditions, the provided standards select motes, known as cache nodes. This scenario can be formulated as:

$$Access\ Time = H * T_c + (1 - H)(T_c - T_m) \quad (3)$$

Here, cache hit ratio is H. Also, T_c, T_m respectively represent the access time, and memory access. The primary role of these cluster heads is to forward the collected data to the destination mote.

IV. RESULT AND DISCUSSION

MATLAB represents a software package employed to investigate the performance of the proposed cache-based WSNs (Wireless Sensor Networks). The suggested protocol is evaluated against current fuzzy logic-assisted WSNs. The proposed protocol's efficiency level is determined by a variety of measures, including the overall packets transferred to the BS and the proportion of inactive nodes.

Table 1 provides the list of the simulations which are done in this work.

TABLE 1: FACTORS FOR SIMULATION

Parameter	Description	Value
A	area of network	(0, 0)–(200, 250)
L-BS	BS location	(150, 250)
N	number of nodes in network	100
$E_{initial}$	initial energy of all nodes	0.5 J
E_{fs}	free space channel model	50 nJ/bit
E_{mp}	multi-path fading channel model	0.0013 pJ/bit/m⁴
d_0	distance threshold	87 m
E_{DA}	data aggregation energy	5 nJ/bit/signal
DP size	data packet size in bit	4000
CP size	control packet size in bit	200

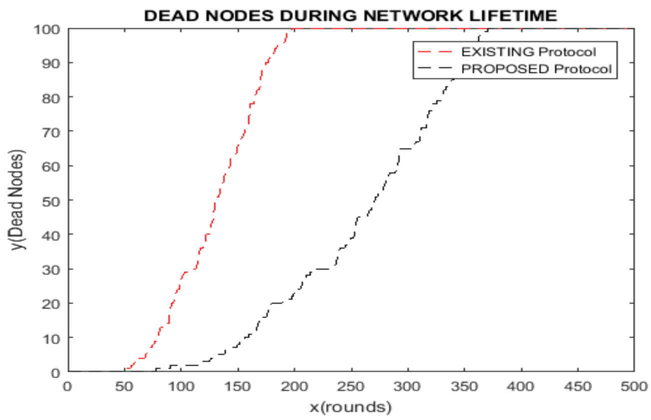

Figure 2. Number of Inactive Nodes

Figure 2 depicts the inactive node counts of the proposed and existing protocols. The standard approach has a dynamic sink. It gathers data from CHs by varying its location from time to time. However, the suggested protocol introduces cache nodes, which enables the sink to obtain information from them. The distribution of cache nodes within the network has a tremendous effect on the decrease of dead nodes.

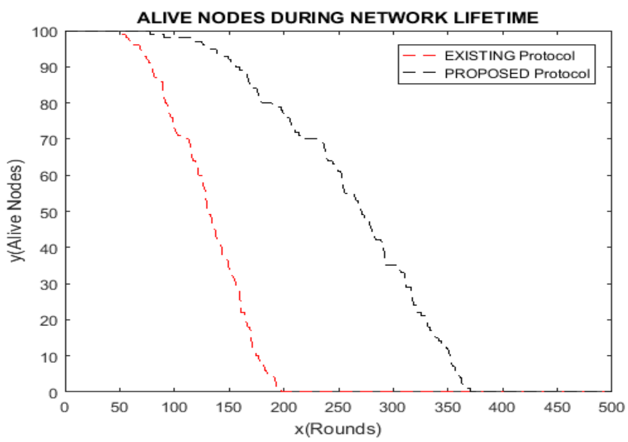

Figure 3: Number of Alive Nodes

Figure 3 depicts the nodes that are alive within the network during different rounds. The objective is to have the maximum number of survived nodes as time passes. In this new protocol, cache nodes are used to bring the overall active nodes up, and the sink is placed near those nodes for data collection. The results offered are a contrast between the author's protocol and the existing one, where it is demonstrated that node longevity has been improved.

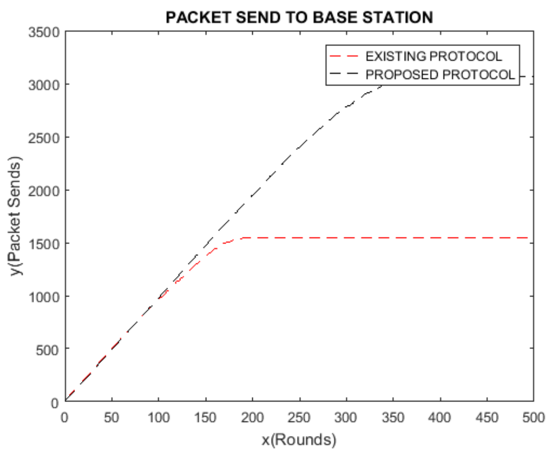

Figure 4: No. of Packets Transferred

Figure 4 depicts how the new protocol compares with the old one w.r.t. the overall packets delivered to the end point. The new protocol has a much better capacity to send a high number of packets as opposed to the conventional ones. In the case of the suggested protocol, the decrease in dead nodes in the network makes the transmission of more packets to the sink possible.

V. CONCLUSION

WSNs (Wireless sensor networks) face significant challenges regarding energy consumption owing to the minute dimension and prevalent placement of sensor nodes. These networks are useful for many applications including object tracking, traffic control, and military operations. To solve the energy efficiency, this research proposes a new modification to the VGDRA protocol that uses caching nodes in the network. The base station collects data from the CHs delivered to these cache nodes. When comparing the revised VGDRA architecture to the classic VGDRA protocol, findings reveal a fifteen percent increase in important indicators like the quantity of inactive nodes, the frequency of living nodes, and the overall number of packets transferred.

REFERENCES

[1] C. R. K. J, V. K. D, M. A. B, B. D and M. A. Majid, "Energy-Efficient Adaptive Clustering and Routing Protocol for Expanding the Life Cycle of the IoT-based Wireless Sensor Network," 6th Int. Conf. Comp. Meth. Com. (ICCMC), Erode, India, 2022, pp. 328-336, doi: 10.1109/ICCMC53470.2022.9753809

[2] S. Umar, N. L. Reddy, T. B. Yadesa, T. D. Deressa and E. Fikadu, "Allocating and Routing Resources in an IoT Network with an Efficient Hybrid Optimization Approach," Int. Con. App. Art. Int. Comp. (ICAAIC), Salem, India, 2022, pp. 1580-1589, doi: 10.1109/ICAAIC53929.2022.9792945

[3] A. Shahraki, A. Taherkordi, Ø. Haugen and F. Eliassen, "A Survey and Future Directions on Clustering: From WSNs to IoT and Modern Networking Paradigms," in IEEE Tran. Net. Ser. Manag., vol. 18, no. 2, pp. 2242-2274, June 2021, doi: 10.1109/TNSM.2020.3035315

[4] V. Vimal et al., "Clustering Isolated Nodes to Enhance Network's Life Time of WSNs for IoT Applications," in IEEE Sys. J., vol. 15, no. 4, pp. 5654-5663, Dec. 2021, doi: 10.1109/JSYST.2021.3103696

[5] G. Kaur, P. Chanak and M. Bhattacharya, "Energy-Efficient Intelligent Routing Scheme for IoT-Enabled WSNs," in IEEE Int. Things J.., vol. 8, no. 14, pp. 11440-11449, 15 July15, 2021, doi: 10.1109/JIOT.2021.3051768

[6] A. Rodríguez, C. Del-Valle-Soto, and R. Velázquez, "Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks Based on Yellow Saddle Goatfish Algorithm," Mathematics, vol. 8, no. 9, p. 1515, Sep. 2020, doi: 10.3390/math8091515

[7] O. O. Ogundile, M. B. Balogun, O. E. Ijiga, and E. O. Falayi, "Energy-balanced and energy-efficient clustering routing protocol for wireless sensor networks," IET Com., vol. 13, no. 10, pp. 1449–1457, Jun. 2019, doi: 10.1049/iet-com.2018.6163

[8] M. Behera, S. K. Mohapatra, P. Mukjerjee and H. K. Sahoo, "Work-In-Progress: DEEC-VD: A Hybrid Energy Utilization Cluster-Based Routing Protocol for WSN for Application in IoT," Int. Conf. Information Technology (ICIT), Bhubaneshwar, Odisha, India, 2017, pp. 97-100, doi: 10.1109/ICIT.2017.42

[9] R. Dogra, S. Rani, H. Babbar, and D. Krah, "Energy-Efficient Routing Protocol for Next-Generation Application in the Internet of Things and Wireless Sensor Networks," Wir. Com. Mob. Comp., vol. 2022, pp. 1–10, Mar. 2022, doi: 10.1155/2022/8006751

[10] M. Micheletti, L. Mostarda and A. Piermarteri, "Rotating Energy Efficient Clustering for Heterogeneous Devices (REECHD)," IEEE 32nd Int. Conf. Ad. Inf. Net. App. (AINA), Krakow, Poland, 2018, pp. 213-220, doi: 10.1109/AINA.2018.00042

[11] A. S. Nandan, S. Singh, R. Kumar and N. Kumar, "An Optimized Genetic Algorithm for Cluster Head Election Based on Movable Sinks and Adjustable Sensing Ranges in IoT-Based HWSNs," in IEEE Int. Things J., vol. 9, no. 7, pp. 5027-5039, 1 April1, 2022, doi: 10.1109/JIOT.2021.3107295

[12] J. T. Thirukrishna, S. Karthik, and V. P. Arunachalam, “Revamp energy efficiency in homogeneous wireless sensornetworks using optimized radio energy algorithm (OREA) and power-aware distance source routing protocol,” Fut. Gen. Comp. Sys., vol. 81, pp. 331–339, 2018, doi: 10.1016/j.future.2017.11.042.

[13] V. Nivedhitha, A. G. Saminathan, and P. Thirumurugan, “DMEERP: a dynamic multi-hop energy efficient routing protocol for WSN,” Microprocessors and Microsystems, vol. 79, pp. 63-70, 2020, doi: 10.1016/j.micpro.2020.103291

[14] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, “A metaheuristic optimization approach for energy efficiency in the IoT networks,” Soft. Pra. Exp., vol. 51, no. 12, pp. 2558–2571, 2021, doi: 10.1002/spe.2797

[15] Y. Fathy and P. Barnaghi, “Quality-based and energy-efficient data communication for the internet of things networks,” IEEE Int. Things J., vol. 6, no. 6, pp. 10318–10331, 2019, doi: 10.1109/JIOT.2019.2938101

[16] M. Elappila, S. Chinara, and D. R. Parhi, “Survivable path routing in WSN for IoT applications,” Per. Mob. Comp., vol. 43, pp. 49–63, 2018, doi: 10.1016/j.pmcj.2017.11.004

[17] A. S. Hampiholi and B. P. Vijaya Kumar, "Efficient routing protocol in IoT using modified Genetic algorithm and its comparison with existing protocols," 2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, 2018, pp. 1-5, doi: 10.1109/CIMCA.2018.8739759.

[18] D. Airehrour, J. A. Gutierrez, and S. K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,” Future Generation Computer Systems, vol. 93, pp. 860–876, Apr. 2019, doi: https://doi.org/10.1016/j.future.2018.03.021.

[19] F. Al-Turjman, “Cognitive routing protocol for disaster-inspired Internet of Things,” Future Generation Computer Systems, vol. 92, pp. 1103–1115, Mar. 2019, doi: https://doi.org/10.1016/j.future.2017.03.014.

[20] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, “Attestation-enabled secure and scalable routing protocol for IoT networks,” Ad Hoc Networks, vol. 98, p. 102054, Mar. 2020, doi: https://doi.org/10.1016/j.adhoc.2019.102054.

[21] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security,” Journal of Information Security and Applications, vol. 52, p. 102467, Jun. 2020, doi: https://doi.org/10.1016/j.jisa.2020.102467.

[22] A. Kumar Dutta et al., “Design of QoS Aware Routing Protocol for IoT Assisted Clustered WSN,” Computers, Materials & Continua, vol. 71, no. 2, pp. 3785–3801, 2022, doi: https://doi.org/10.32604/cmc.2022.023657.

[23] M. Shafiq et al., “Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN,” Computers, Materials & Continua, vol. 67, no. 3, pp. 3505–3521, 2021, doi: https://doi.org/10.32604/cmc.2021.015533.

[24] S. Sennan, Kirubasri, Y. Alotaibi, D. Pandey, and S. Alghamdi, “EACR-LEACH: Energy-Aware Cluster-based Routing Protocol for WSN Based IoT,” Computers, Materials & Continua, vol. 72, no. 2, pp. 2159–2174, 2022, doi: https://doi.org/10.32604/cmc.2022.025773.

[25] Naveen Kumar Gupta, Rama Shankar Yadav, Rajendra Kumar Nagaria, D. Gupta, Achyut Mani Tripathi, and Om Jee Pandey, “Anchor-based void detouring routing protocol in three dimensional IoT networks,” Computer Networks, vol. 227, pp. 109691–109691, Mar. 2023, doi: https://doi.org/10.1016/j.comnet.2023.109691.

[26] H. Gul, S. Ullah, K.-I. Kim, and F. Ali, “A Traffic-Aware and Cluster-Based Energy Efficient Routing Protocol for IoT-Assisted WSNs,” Computers, materials & continua/Computers, materials & continua (Print), vol. 80, no. 2, pp. 1831–1850, Jan. 2024, doi: https://doi.org/10.32604/cmc.2024.052841