ISSN 2455 – 9091

IJCSET JANUARY Volume 11 Issue 1

International Journal of Computer Science Engineering and Technology (IJCSET)

https://www.doi.org/10.5281/zenodo.10566804

NOVEL ENERGY BASED ROUTING MECHANISM FOR WSN BASED IoT APPLICATIONS

[1] Mr. A. Arun Joseph, [2] Mr. C. Prakash,
[1, 2] Assistant Professor,
[1] Department of Computer Applications, [2] Department of Computer Technology,
[1] Navarasam Arts and Science College for Women, [2] Nandha Arts and Science College,
[1] Erode – 638101, [2] Erode - 638052.

ABSTRACT: - The term "Internet of Things," or "IoT," was created to describe a network of physically connected, interconnected objects that are equipped with sensors and network connectivity so they can gather, process, and share data. The term "things" in the context of the Internet of Things encompasses a broad range of devices, including biochip transponders, heart monitoring implants, weather monitoring sensors, internet-connected home appliances, cars equipped with sensors, and any other item possessing an IP address and the capability to transmit data across a network. The barrier separating information technology and operational technology has been breached by the convergence of wireless technologies, micro-electromechanical systems, and the internet. This enables unstructured data produced by machines to be transferred over a network and analyzed. The primary obstacle associated with the Internet of Things is energy management, as energy powers every device, network, and application. One of the primary issues with WSNs is routing, for which numerous solutions have been created. The intricacies of sensor networks and the consequences of wireless communication present numerous obstacles to ensuring effective routing. In this work, a novel routing methodology is employed to prevent energy waste, and the suggested method both uses and harvests energy.

Keywords: - Internet of Things, Energy Efficient, Wireless Sensor Network, Routing.

1. INTRODUCTION

The term “Internet of Things” (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors. Ashton coined the term to illustrate the power of connecting Radio-Frequency Identification (RFID) used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention [1]. Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items.

While the term “Internet of Things” is relatively new, the concept of combining computers and networks to monitor and control devices has been around for decades. By the late 1970s, for example, systems for remotely monitoring meters on the electrical grid via telephone lines were already in commercial use. In the 1990s, advances in wireless technology allowed “machine–to–machine” (M2M) enterprise and industrial solutions for equipment monitoring and operation to become widespread. Many of these early M2M solutions, however, were based on closed purpose–built networks and proprietary or industry–specific standards, rather than on Internet Protocol (IP)–based networks and Internet standards [4].

IoT should have the capability to connect and transfer data among billions and trillions of devices. For this to happen seamlessly, it is critical to have a layered architecture in place. The architecture should be highly scalable and flexible to accommodate the wide gamut of components and technologies that form a part of the IoT ecosystem.

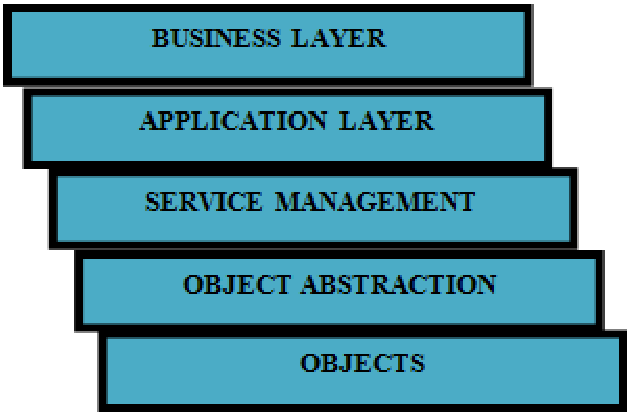

Figure 1: - Layered architecture of IoT

- **Objects layer**, also known as devices layer, comprises the physical devices that are used to collect and process information from the IoT ecosystem. Physical devices include different types of sensors such as those that are typically based on micro-electromechanical systems (MEMS) technology. Sensors could be optical sensors, light sensors, gesture and proximity sensors, touch and fingerprint sensors, pressure sensors, and more.
- **Object abstraction layer** transfers data that are collected from objects to service management layer using secure transmission channels. Data transmission can happen

using any of the following technologies like, RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth low energy, Infrared, ZigBee. Specialized processes for handling functions such as cloud computing and data management are also present in this layer.

➢ **The service management layer** acts as middleware for the IoT ecosystem. This layer pairs specific services to its requester based on addresses and names. This layer provides flexibility to the IoT programmers to work on different types of heterogeneous objects irrespective of their platforms. This layer also processes the data that are received from the object abstraction layer. After data processing, necessary decisions are taken about the delivery of required services, which are then done over network wire protocols.

➢ **Application layer** provides the diverse kinds of services requested by the customer. The type of service requested by the customer depends on the specific use case that is adopted by the customer.

➢ **Business layer** performs the overall management of all IoT activities and services. This layer uses the data that are received from the network layer to build various components such as business models, graphs, and flowcharts. This layer also has the responsibility to design, analyze, implement, evaluate, and monitor the requirements of the IoT system. This layer has the capability to use big data analysis to support decision-making activities. This layer also performs a comparison of obtained versus expected outputs to enhance the quality of services.

The building blocks of IoT are sensory devices, remote service invocation, communication networks, and context-aware processing of events; these have been around for many years [7]. However, what IoT tries to picture is a unified network of smart objects and human beings responsible for operating them (if needed), who are capable of universally and ubiquitously communicating with each other.

2. LITERATURE REVIEW

Binu, G. S., & Shajimohan, B. (2020) analyzed that Wireless Sensor Network (WSN) is used in many applications for different roles, such as monitoring, data transmitting, and information gathering, and so on [2]. However, managing energy in WSN is a critical task. To end this issue several clustering and heuristic strategies were constructed still, a suitable solution is not found. So the author's research proposed a novel African Buffalo based Two Tier Data Dissemination (AB-TTDD) strategy to monitor the energy drained node in an earlier stage before the data transmission. The fitness function of African Buffalo model is utilized to recognize the harmful and energy drained nodes in an earlier stage. Furthermore, they introduced a novel Temporary Energy Mapping Algorithm (TEMA) is developed to maintain the route by creating the reference node instead of energy drained node. This novel proposed mechanism has reduced the packet flow ratio and power consumption in a high manner. At the same time, it enhanced the energy intensity of sensor hubs by mounting its lifetime and affording the reroute. Subsequently, the capability of the proposed strategy is validated with the recent research works and achieved better performance by reducing energy consumption and packet drop ratio.

Deebak, B. D., & Al-Turjman, F. (2020) finds that Internet of Things (IoT) has advanced its pervasiveness across the globe for the development of smart networks [3]. In IoT applications, the edge computing exploits distributed architecture and closeness of end-users to provide faster response and better quality of service. However, the security concern is majorly addressed to resist the vulnerability of attacks (VoA). The author's proposed a secure routing and monitoring protocol with multi-variant tuples using Two-Fish (TF) symmetric key approach to discover and prevent the adversaries in the global sensor network. The proposed approach is designed on the basis of the Authentication and Encryption Model (ATE). Using Eligibility Weight Function (EWF), the sensor guard nodes are selected and it is hidden with the help of complex symmetric key approach. A secure hybrid routing protocol is chosen to be built by inheriting the properties of both Multipath Optimized Link State Routing (OLSR) and Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols. The result of the proposed approach is shown that it has a high percentage of monitoring nodes in comparison with the existing routing schemes.

Han, B., et al., (2022) addressed problem of their limited energy, the communication abilities of the wireless nodes distributed in the WSN are limited [5]. The main task of WSNs is to collect more data from targets in an energy-efficient way, because the battery replacement of large amounts of nodes is a labor-consuming work. The author's introduced an adaptive hierarchical-clustering-based routing protocol for EH-WSNs (HCEH-UC) is proposed to achieve uninterrupted coverage of the target region through the distributed adjustment of the data transmission. Firstly, a hierarchical-clustering-based routing protocol is proposed to balance the energy consumption of nodes. Then, a distributed alternation of working modes is proposed to adaptively control the number of nodes in the energy-harvesting mode, which could lead to uninterrupted target coverage. The simulation experimental results verify that the proposed HCEH-UC protocol can prolong the maximal lifetime coverage of WSNs compared with the conventional routing protocol and achieve uninterrupted target coverage using energy-harvesting technology.

Nagaraju, R., et al., (2022) finds the solution for nodes generally function with limited battery units and, hence, energy efficiency is considered as the main design challenge [6]. For homogeneous WSNs, several routing techniques based on clusters are available, but only a few of them are focused on energy-efficient heterogeneous WSNs (HWSNs). This research work presents an energy optimizing secure routing scheme for IoT application in heterogeneous WSNs. In our proposed scheme, secure routing is established for confidential data of the IoT through sensor nodes with heterogeneous energy using the multipath link routing protocol (MLRP). After establishing the secure routing, the energy and network lifetime is improved using the hybrid-based TEEN (H-TEEN) protocol, which also has load balancing capacity. Furthermore, the data storage capacity is improved using the ubiquitous data storage protocol (U-DSP). This routing protocol has been implemented and compared with two other existing routing protocols, and it shows an improvement in performance parameters such as throughput, energy efficiency, end-to-end delay, and network lifetime and data storage capacity.

3. IoT ARCHITECTURES

When talking about a distributed environment, interconnectivity among entities is a critical requirement, and IoT is a good example. Holistic system architecture for IoT needs to guarantee flawless operation of its components (reliability is considered as the most import design factor in IoT) and link the physical and virtual realms together. To achieve this, careful consideration is needed in designing failure recovery and scalability [8]. Additionally, since mobility and dynamic change of location has become an integral part of IoT systems with the widespread use of smart phones, state-of-the-art architectures need to have a certain level of adaptability to properly handle dynamic interactions within the whole ecosystem.

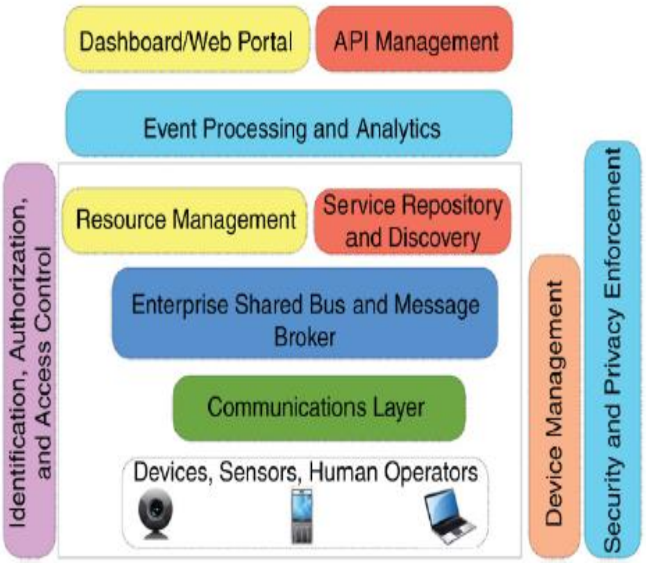
Dashboard/Web Portal
API Management
Event Processing and Analytics
Resource Management
Service Repository and Discovery
Enterprise Shared Bus and Message Broker
Communications Layer
Devices, Sensors, Human Operators
Identification, Authorization, and Access Control
Device Management
Security and Privacy Enforcement

Figure 2: - Architecture of IoT

Different service and presentation layers are shown in this architecture. Service layers include event processing and analytics, resource management and service discovery, as well as message aggregation and Enterprise Service Bus (ESB) services built on top of communication and physical layers. API management, which is essential for defining and sharing system services and web-based dashboards (or equivalent Smartphone applications) for managing and accessing these APIs, are also included in the architecture [9].

Due to the importance of device management, security and privacy enforcement in different layers and the ability to uniquely identify objects and control their access level, these components are prestressed independently in this architecture.

3.1. SOA Based Architecture

In IoT, service-oriented architecture (SOA) might be imperative for the service providers and users. SOA ensures the interoperability among the heterogeneous devices. SOA consisting of four layers, with distinguished functionalities as follows:

- Sensing layer is integrated with available hardware objects to sense the status of things
- Network layer is the infrastructure to support over wireless or wired connections among things.
- Service layer is to create and manage services required by users or applications
- Interfaces layer consists of the interaction methods with users or applications.

Generally, in such architecture a complex system is divided into subsystems that are loosely coupled and can be reused later (modular decomposability feature), hence providing an easy way to maintain the whole system by taking care of its individual components. This can ensure that in the case of a component failure the rest of the system (components) can still operate normally [10].

SOA has been intensively used in WSN, due to its appropriate level of abstraction and advantages pertaining to its modular design.

3.2. API-Oriented Architecture

APIs for IoT applications helps the service provider attract more customers while focusing on the functionality of their products rather than on presentation. In addition, it is easier to enable multitenancy by the security features of modern Web APIs such as OAuth, APIs which indeed are capable of boosting an organization's service exposition and commercialization. It also provides more efficient service monitoring and pricing tools than previous service-oriented approaches.

3.3. Communication Protocols

Seamless connectivity is a key requirement for IoT. Network-communication speed, reliability, and connection durability will impact the overall IoT experience.

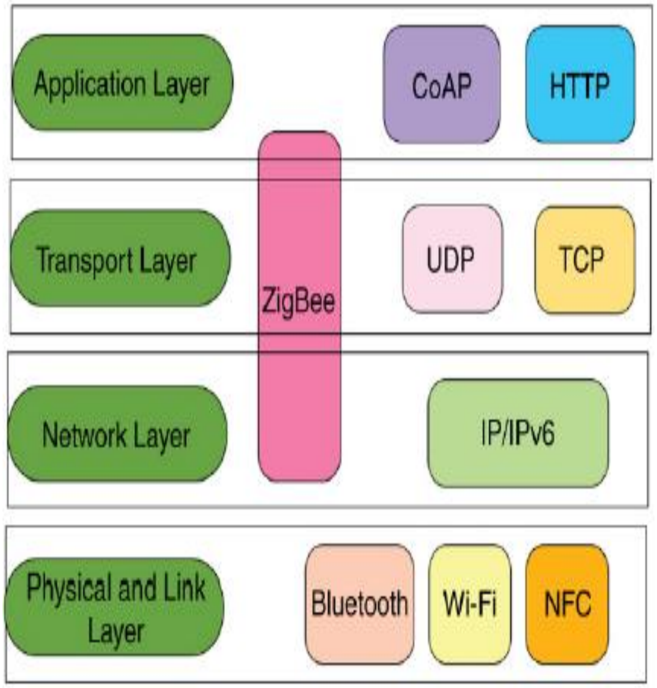

Figure 3: - IoT Communication Protocols

ISSN 2455 – 9091

3.3.1. Network Layer

Based on the device's specification (memory, CPU, storage, battery life), the communication means and protocols vary. However, the commonly used communication protocols and standards are listed below:

- RFID
- IEEE 802.11
- Low-power Wireless Personal Area Networks (6LoWPAN) standards by IEFT
- M2M protocols such as MQTT and CoAP
- IP layer technologies, such as IPv4, IPv6, etc.

3.3.2. Transport and Application Layer

Segmentation and poor coherency level, which are results of pushes from individual companies to maximize their market share and revenue, has made developing IoT applications cumbersome [11]. Universal applications that require one-time coding and can be executed on multiple devices are the most efficient.

Protocols in IoT can be classified into three categories:

- General-purpose protocols like IP and SNMP that have been around for many years and are vastly used to manage, monitor, configure network devices, and establish communication links;
- Lightweight protocols such as CoAP that have been developed to meet the requirements of constrained devices with tiny hardware and limited resources;
- Device- or vendor-specific protocols and APIs that usually require a certain build environment and toolset.

Selecting the right protocols at the development phase can be challenging and complex, as factors such as future support, ease of implementation, and universal accessibility have to be considered.

Additionally, thinking of other aspects that will affect the final deployment and execution, like required level of security and performance, will add to the sophistication of the protocol-selection stage [16].

4. EXISTING SYSTEM & ITS DIFFICULTIES

The nodes have wireless connectivity and harvest energy from ambient energy sources. The data sink is powered by an unlimited energy supply. In this model, the nodes can be either a sensor or a router. As a sensor node, it generates a data packet to transmit to the sink, and as a router it forwards the packet to the sink via the links that connect sensors and routers.

A sensor can operate as a router to assist other sensors in forwarding packets to the sink. In this work, we consider three typical renewable energy sources, such as: solar, vibration (e.g, moving vehicles) and RF radiation. All nodes can harvest energy from one of these sources with different arrival energy harvesting rates [12].

To manage the incoming energy, we consider the harvest store-use protocol that allows a node to store electricity energy. If the harvested energy is higher than the node's energy consumption, the excess energy will be stored for later use.

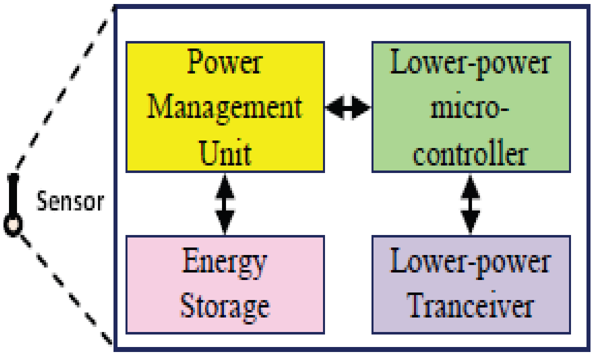

Figure 4: - Existing System Node Configuration

In order to design an effective routing protocol, it is necessary to determine the energy consumed by each node to process a packet. This energy consists of the energy required to transmit, receive or forward the packet on the selected path. In addition, the node has to expend energy to listen for an arrival packet or wait for an incoming event. In the IEEE 802.15.4-based WSNs, the media access control (MAC) sub layer will control nodes to enter into these above operating modes.

The energy harvesting activity can be treated as a stochastic process due to the random nature of ambient energy sources. Assume that the energy harvesting process is independent of the four operating modes (e.g., transmitting, receiving, idle-listening and sleeping) of the nodes. To improve the knowledge of the arrival energy in the harvesting process, it is necessary to develop an energy prediction model. In this work, we adopt the prediction model based on a standard Kalman filter (KF). The Kalman filter is a recursive algorithm that uses only the estimated state from the previous time step and the current measurement are needed to compute the estimate for the current state. It minimizes the mean square of the estimation error under white noise [13].

The main disadvantages of the existing system are summarized as follows:

- We jointly address the issues of EE and QoS for IoT applications by developing an energy-harvesting aware routing protocol that is operated at the network layer of IEEE 802.15.4-based networks. The proposed algorithm can adapt to the varying traffic load from the IoT applications, the residual energy and the arrival harvesting energy at sensor nodes,
- We propose an energy prediction model for the arrival harvested energy at the sensor nodes. The stochastic characteristics of the ambient energy sources are taken into account in the model,
- We introduce a new parameter termed as 'extra backoff', which can be integrated into the proposed routing algorithm. Based on a combination of the 'extra backoff' and the energy prediction process, we define the cost metric which can be used to build the routing table and to select the best routes for packet forwarding.

5. PROPOSED SYSTEM & ITS CONTRIBUTION

An adaptive scheduling algorithm is evaluated. The work combines the topology and routing improvements with management, synchronization and scheduling techniques.

In an appropriate routing scheme, a lot of random depletion schemes of wireless sensors are reduced and partitioned into grid layouts. In [14] the authors propose a direct grid topology from the source node to the sink node. The sensor network is divided in grid subnets where the transmitter node is selected according to its dependencies on a certain cost parameter that includes the distance to the location of the ideal grid node and the residual power. In a non-uniform grid-based coordinated routing design is presented. Here are used different types of partitioned square shaped grids that divide the sensor network. A load balancing with respect to the residual energy is also implemented.

Some studies are made on a classic grid topology where the nodes are arranged on an array layout and all of them participate to route data. In a comparison between four routing algorithms for grid topologies is presented. A similar topology is proposed in this paper but the data is transmitted accordingly with the residual energy of the nodes [15].

The routes are structured on an adaptive format, considering the leveling of energy spent. It is also studied the influence on the network lifetime of the sink position in a grid WSN. In addition, by taking into account a certain degree of spatial and temporal correlation, a data aggregation technique was proposed in order to increase the network lifetime.

We are interested to study a deployment of the wireless sensor nodes in a situation where the nodes respect the places of an array. They are placed manually at certain locations where the distance between two neighboring nodes is the same (d). The sensor network has a MXN dimension and is similar with the one presented in Fig. 1. Each sensor is identified by its bi-dimensional coordinates, (i, j), where i represents the horizontal index of the sensor with values between 0, M-1 and j represents the vertical index of the sensor taking values between 0, N-1.

For the simplicity of the presentation we choose to select the network sink at the point (0,0). The sink also acts like a sensor and it has unlimited energy. Each node placed in the interior of the grid has 4 neighbors: two high neighbors, node (i, j + 1) and node (i + 1, j), and two low neighbors, node (i - 1, j) and node (i, j – 1). The nodes located on the edge of the grid can have two or three neighbors. A node can transmit only through the smallest paths, to his low neighbors (Fig. 5). This way the nodes closer to the sink are more used because they transmit all the data from behind.

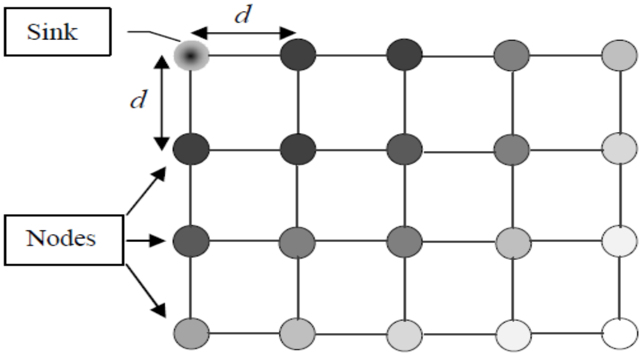

Figure 5: - Structure of the Proposed Work

In a grid WSN the nodes closer to the sink spent the most amount of energy. It is considered that the network lifetime is the same with the lifetime of the first node that dies. Assuming ideal conditions where all the data packets have equal sizes and the transmission is without error, in order to balance the data traffic and to maximize the lifetime of the network, the nodes that have two options in transmitting will choose alternate destination.

CONCLUSION

This study proposes an energy optimization technique with safe routing for heterogeneous WSN applications in the Internet of Things. This dependable and safe routing protocol collects information from nearby nodes at the base station and creates an energy-saving key and multipath for each node. In order to select new pathways and CHs, CHs assist in data aggregation and pass the data to BS, which is always checking nodes for leftover energy. The integrated implementation of proposed work produced a minimum end-to-end delay in suitable data packets and reduced the energy consumption at SNs by leveraging the complexity of multimedia processing and the aggregation process to the CHs side and avoiding path loops and path cycles for route establishment.

REFERENCES

[1]. Al-Hubaishi, M., Çeken, C., & Al-Shaikhli, A. (2019). A novel energy-aware routing mechanism for SDN-enabled WSAN. International Journal of Communication Systems, 32(17), e3724.

[2]. Binu, G. S., & Shajimohan, B. (2020). A novel heuristic based energy efficient routing strategy in wireless sensor network. Peer-to-Peer Networking and Applications, 13, 1853-1871.

[3]. Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, 102022.

[4]. Ilyas, M., Ullah, Z., Khan, F. A., Chaudary, M. H., Malik, M. S. A., Zaheer, Z., & Durrani, H. U. R. (2020). Trust-based energy-efficient routing protocol for Internet of things–based sensor networks. International Journal of Distributed Sensor Networks, 16(10), 1550147720964358.

[5]. Han, B., Ran, F., Li, J., Yan, L., Shen, H., & Li, A. (2022). A novel adaptive cluster based routing protocol for energy-harvesting wireless sensor networks. Sensors, 22(4), 1564.

[6]. Nagaraju, R., Goyal, S. B., Verma, C., Safirescu, C. O., & Mihaltan, T. C. (2022). Secure routing-based energy optimization for IOT application with heterogeneous wireless sensor networks. Energies, 15(13), 4777.

[7]. Haseeb, K., Ud Din, I., Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. Sensors, 20(7), 2081.

[8]. Bhargava, D., Prasanalakshmi, B., Vaiyapuri, T., Alsulami, H., Serbaya, S. H., & Rahmani, A. W. (2022). CUCKOO-ANN based novel energy-efficient optimization technique for IoT sensor node modelling. Wireless Communications and Mobile Computing, 2022, 1-9.

[9]. Dogra, R., Rani, S., Sharma, B., Verma, S., Anand, D., & Chatterjee, P. (2021). A novel dynamic clustering approach for energy hole mitigation in Internet of Things-based wireless

sensor network. International Journal of Communication Systems, 34(9), e4806.

[10]. Mishra, M., Gupta, G. S., & Gui, X. (2021). Network Lifetime Improvement through Energy-Efficient Hybrid Routing Protocol for IoT Applications. Sensors, 21(22), 7439.

[11]. Kaur, G., Chanak, P., & Bhattacharya, M. (2021). Energy-efficient intelligent routing scheme for IoT-enabled WSNs. IEEE Internet of Things Journal, 8(14), 11440-11449.

[12]. Avdhesh Yadav, S., & Poongoodi, T. (2022). A novel optimized routing technique to mitigate hot-spot problem (NORTH) for wireless sensor network-based Internet of Things. International Journal of Communication Systems, 35(16), e5314.

[13]. Senthil, G. A., Raaza, A., & Kumar, N. (2022). Internet of things energy efficient cluster-based routing using hybrid particle swarm optimization for wireless sensor network. Wireless Personal Communications, 122(3), 2603-2619.

[14]. Rajeswari, A. R., Kulothungan, K., Ganapathy, S., & Kannan, A. (2021). Trusted energy aware cluster based routing using fuzzy logic for WSN in IoT. Journal of Intelligent & Fuzzy Systems, 40(5), 9197-9211.

[15]. Dogra, R., Rani, S., Shafi, J., Kim, S., & Ijaz, M. F. (2022). ESEERP: Enhanced smart energy efficient routing protocol for internet of things in wireless sensor nodes. Sensors, 22(16), 6109.

[16]. Hassan, A. A. H., Shah, W. M., Habeb, A. H. H., Othman, M. F. I., & Al-Mhiqani, M. N. (2020). An improved energy-efficient clustering protocol to prolong the lifetime of the WSN-based IoT. Ieee Access, 8, 200500-200517.