IJASRM

International Journal of Advanced Scientific Research and Management, Volume 7 Issue 9, Sept 2023

www.ijasrm.com

ISSN 2455-6378

Comprehensive Review of Routing Protocol in a Wireless Sensor Network for an IOT Applications

A.Geetha[1], Dr.S.Karthigai Lakshmi[2]

[1,2] Department of Electronics And Communication Engineering, SSM Institute Of Engineering And Technology, Dindigul, TamilNadu, India

[2] Department of Electronics And Communication Engineering, SSM Institute Of Engineering And Technology, Dindigul, TamilNadu, India

Abstract

The Internet of Things (IoT) has proved to be an interesting and promising paradigm that aims to contribute to countless applications by connecting more physical "things" to the Internet.The convergence of the Internet of Things (IoT) and Wireless Sensor Networks (WSNs) has enabled the proliferation of interconnected smart devices that gather and exchange vast amounts of data. The efficient and reliable routing of this data in such networks is crucial to ensuring seamless communication among devices. Wireless Sensor Networks (WSNs) are a fundamental component of Internet of Things (IoT) applications, enabling the collection and transmission of data from various sensors in real-time. Effective data routing is critical to ensure reliable and efficient communication within these networks. In this review, we analyze and compare different routing protocols used in WSNs for IoT applications. We explore their characteristics, strengths, and weaknesses in handling the unique challenges posed by IoT environments. Through this comprehensive review, we aim to provide insights into the state-of-the-art in WSN routing for IoT and identify potential areas for future research and improvements.

Keywords: *Internet of Things (IoT), Routing protocols, Wireless Sensor Networks (WSN)*

1. Introduction

IoT is the Internet of Things.An internet of things (IoT) is a substantial regional configuration that is linked to the standard characteristics of a traditional system that may connect and exchange data. IoT also known as the "internet of everything, it is a new paradigm that connects the physical and digital worlds via a network of sensors, computers, the internet, radio frequency identification (RFID), embedded systems and communication technology . Nowadays, sensor networks have gained considerable popularity due to their flexibility in monitoring the physical world that can detect, process, and convey. Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) have emerged as transformative technologies that are reshaping the way we interact with the world around us. WSNs, consisting of small, autonomous sensor nodes equipped with sensing, computation, and communication capabilities, enable the collection of data from the physical environment. IoT, on the other hand, connects various smart devices and systems, enabling seamless data exchange and intelligent decision-making.IoT applications often involve a large number of heterogeneous devices, variable network topologies, dynamic mobility patterns, limited resources, and diverse data traffic patterns. As a result, routing protocols must be able to adapt to these complexities and provide efficient data delivery while conserving energy and ensuring reliable communication.

The successful integration of WSNs into IoT applications requires routing protocols that can handle the unique challenges presented by these environments .Routing protocols are a fundamental component of WSNs that determine how data packets are efficiently and reliably forwarded from source nodes to destination nodes within the network.It plays a crucial role in determining the path that data packets take from source nodes to destination nodes in WSNs. In the context of IoT applications, where a vast number of interconnected devices are involved, the design and performance of routing protocols become even more critical.The rapid growth of the Internet of Things (IoT) and the widespread adoption of Wireless Sensor Networks (WSNs) have significantly impacted various industries and domains, ranging from smart cities and environmental monitoring to healthcare and industrial automation. As the number of IoT devices and WSNs continues to escalate, the efficient and reliable routing of data within these networks becomes increasingly vital.

Routing protocols play a critical role in enabling data transmission and communication within IoT-enabled Wireless Sensor Networks (WSNs).

https://doi.org/10.36282/IJASRM/8.9.2023.1902

1.Data Collection and Aggregation

In IoT-enabled WSNs, numerous sensor nodes are deployed to collect data from the physical world. These nodes are typically resource-constrained in terms of processing power, memory, and energy. Routing protocols determine how data is collected from these nodes and forwarded to a central point, often referred to as a sink or gateway.

2. Energy Efficiency

Energy efficiency is a critical concern in WSNs, as many sensor nodes are battery-powered and may be deployed in remote or inaccessible locations. Efficient routing protocols are essential to prolong the network's lifespan by minimizing energy consumption.

3. Scalability

IoT applications often involve large-scale deployments with a vast number of sensor nodes. Routing protocols must be scalable to handle networks of varying sizes.

4. Data Reliability

Many IoT applications require reliable data transmission, particularly in critical applications like healthcare monitoring, industrial automation, or environmental sensing.

5. Security

IoT-enabled WSNs are susceptible to various security threats, including data interception, tampering, and denial of service attacks. Routing protocols can include security mechanisms to protect data transmission.

2. Wireless Sensor Networks and IoT Applications

2.1Overview of WSNs

Wireless Sensor Networks (WSNs) are an emerging and interdisciplinary field that combines wireless communication, sensor technology, and data processing. WSNs are composed of small, low-cost devices called sensor nodes, equipped with sensors to gather data from the environment and wireless communication capabilities to transmit the collected data to a central location, often called a base station or sink. These nodes are typically autonomous and have limited processing, storage, and energy resources. The sensor nodes are equipped with various sensing capabilities, such as temperature, humidity, light, pressure, and motion, allowing them to observe changes in their surroundings.The development and deployment of WSNs have been driven by advancements in microelectronics, wireless communication technologies, and the growing demand for cost-effective and scalable solutions for real-world applications.

2.1.1 Key Components of WSNs

a).Sensor Nodes: The fundamental building blocks of WSNs are sensor nodes, which are typically small, low-cost devices with limited processing power and memory. Each node is equipped with sensors, a microcontroller, a radio transceiver, and a power source (e.g., batteries or energy harvesting).

b)Communication: Sensor nodes in WSNs communicate wirelessly with each other to form a self-organizing and self-configuring network.. They can either transmit data directly to a central base station or relay data through other nodes to reach the destination, forming a multi-hop network.

c).Base Station or Sink: The base station, also known as the sink, serves as the central point of communication and data aggregation in the WSN. It collects data from sensor nodes, processes it, and possibly forwards it to external networks or applications.

d)Network Topology: The network topology of a WSN can vary depending on the application requirements and deployment scenarios. Common topologies include star, tree, mesh, and cluster-based topologies.

e)Ad hoc Networking: WSNs use ad hoc networking, meaning the nodes can dynamically establish and maintain connections with neighboring nodes without relying on a pre-existing infrastructure. This makes WSNs suitable for dynamic and rapidly changing environments.

2.1.2 Challenges of WSN in IoT

Wireless Sensor Networks (WSNs) face specific challenges when integrated into the broader Internet of Things (IoT) ecosystem. The integration of WSNs with IoT introduces new complexities and requirements due to the large-scale deployment, diverse device types, and heterogeneous communication protocols.

Interoperability: IoT encompasses a wide range of devices and communication technologies, making it crucial to ensure interoperability between different WSN devices and IoT platforms. Standardization efforts like IoT protocols (e.g., MQTT, CoAP) play a vital role in addressing this challenge.

Resource Constraints: WSN nodes are resource-constrained devices with limited processing power, memory, and energy supply. IoT applications often demand real-time data processing and analysis, which can strain the resources of WSN nodes.

Energy Efficiency: Energy efficiency is a critical concern for WSN nodes, as they are often battery-powered and may be deployed in remote or hard-to-reach locations. Optimizing energy consumption in WSNs is essential to prolong the operational lifetime of devices.

Data Security and Privacy: IoT applications involve the collection, transmission, and storage of sensitive data. Ensuring data security and privacy in WSNs becomes crucial to prevent unauthorized access, data tampering, and privacy breaches.

Network Heterogeneity: IoT applications consist of various networks with different communication technologies (e.g., Zigbee, Bluetooth, Wi-Fi, LPWAN). Integrating these heterogeneous networks and managing seamless communication is a challenge.

Data Management and Analytics: Managing the vast amount of data generated by IoT devices requires

https://doi.org/10.36282/IJASRM/8.9.2023.1902

efficient data storage, processing, and analytics. WSNs need to support data aggregation and filtering techniques to reduce the data load on the network.

Mobility Support: Some IoT devices, such as wearables or smart vehicles, may be mobile. Supporting seamless communication and data handover as these devices move between different network areas is a challenge.

Reliability and Fault Tolerance: IoT applications often require high reliability and fault tolerance. WSNs must be resilient to node failures and communication disruptions to ensure continuous operation.

Overhead and Latency: IoT applications with stringent latency requirements demand low communication overhead and reduced end-to-end latency. Balancing these requirements with resource constraints in WSNs is a challenge.

Quality of Service: All heterogeneous IoT devices must contribute to the quality of service provided to sensor nodes in terms of intelligence. Thisheterogeneous device allows for task distribution amongst nodes with resources available. Due to changeable network setups andconnection properties, the current QoS techniques available on the Internet still require enhancement

2.1.3 Role of WSNs in Supporting IoT:

WSNs play a crucial role in supporting the Internet of Things (IoT) by acting as the underlying infrastructure for data collection and transmission. They serve as the "sensory nervous system" of IoT applications, providing a seamless connection between the physical world and the digital realm.

Data Collection: WSNs are responsible for gathering real-time data from various sensors distributed in the environment. These sensors continuously monitor physical parameters, and the collected data is then processed and sent to the central IoT platform.

Real-time Monitoring: WSNs enable real-time or near-real-time monitoring of the physical environment. The data collected by the sensors can be instantly transmitted to the central control system or cloud-based IoT platform, allowing users to make informed decisions and respond promptly to changes.

Autonomous Operation: WSNs are capable of autonomous operation and self-organization. They can dynamically adjust their network topology, optimize routing paths, and adapt to changes in the environment without human intervention.

Data Fusion and Aggregation: WSNs employ data fusion and aggregation techniques to minimize redundant data and reduce communication overhead. This ensures efficient data transmission and utilization of network resources.

Integration with IoT Platforms: WSNs interface with cloud-based IoT platforms where data is stored, analyzed, and processed. This integration allows for advanced data analytics, predictive modeling, and actionable insights.

2.1.4 Applications of IoT based WSN

Wireless Sensor Networks (WSNs) have a wide range of applications in diverse domains due to their ability to monitor, collect, and transmit data from the physical environment in a cost-effective and efficient manner.

Environmental Monitoring: IoT-based WSNsare extensively used for environmental monitoring in smart cities and rural areas. They can measure parameters such as air quality, temperature, humidity, noise levels, and pollution levels. This data is crucial for urban planning, resource management, and environmental conservation.

Smart Agriculture: In smart agriculture, IoT-based WSNs provide real-time data on soil moisture levels, temperature, humidity, and crop health. Farmers can use this data to optimize irrigation, fertilization, and pest control, leading to increased crop yield and efficient resource utilization.

Healthcare and Medical Monitoring: WSNs integrated with IoT enable healthcare settings for remote patient monitoring, continuous monitoring of vital signs, and tracking patient activities telemedicine applicationsThis enables healthcare professionals to provide personalized care, detect anomalies, and improve patient outcomes.

Industrial Automation IoT-based WSNsplay a vital role in industrial automation and control systems. They monitor equipment, machinery, and manufacturing processes, providing real-time data to optimize production, reduce downtime, predictive maintenance, worker safetyand enhance overall efficiency.

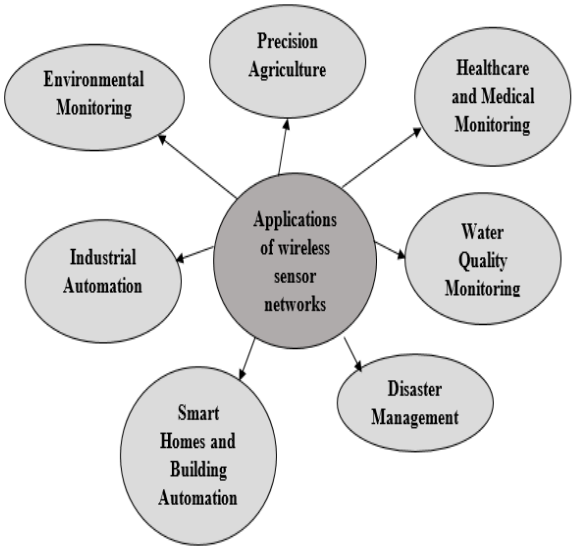

Fig:1 Applications of IoT based WSN

Smart Homes and Building Automation:IoT-based WSNs in smart homes and buildings to enable home automation, energy management, and security. Sensor nodes can detect occupancy, control lighting, heating, and cooling systems, and provide security surveillance.

https://doi.org/10.36282/IJASRM/8.9.2023.1902

Structural Health Monitoring:IoT-based WSNs can be deployed to monitor the health of infrastructure like bridges, buildings, and dams. By detecting vibrations, strain, and deformation, they help in identifying potential structural issues and ensuring public safety.

Wildlife Conservation: WSNs combined with IoT technology aid in wildlife tracking, habitat monitoring, and anti-poaching efforts. These networks offer real-time data on animal movement and behavior, helping conservationists protect endangered species..

Disaster Management:IoT-based WSNs can be deployed for early warning systems, detecting seismic activities, floods, earthquakes and other natural disasters. This data helps in timely evacuation and disaster preparedness.

Traffic Management: IoT-based WSNs can be used for intelligent traffic management by monitoring traffic flow, congestion, and vehicle density. This data helps optimize traffic signal timings and improve overall transportation efficiency.

Military and Defense Applications: IoT-based WSNs find applications in military and defense for surveillance, reconnaissance, border security, and battlefield monitoring.

Water Quality Monitoring: WSNs monitor water quality in rivers, lakes, and reservoirs, assessing parameters like pH, dissolved oxygen, and contaminants. This data aids in water resource management and conservation.

Asset Tracking and Logistics: IoT-based WSNs enable real-time tracking of assets and shipments in logistics and supply chain management. They provide visibility into the movement and condition of goods, improving efficiency and reducing losses

Precision Livestock Farming: WSNs combined with IoT are utilized in precision livestock farming to monitor animal health, behavior, and location. This data enhances animal welfare and productivity in the agriculture sector.

Oil and Gas Industry: In the oil and gas sector, IoT-based WSNs monitor and control remote equipment and pipelines, ensuring operational safety and efficiency in challenging environments.

3. Classification of Routing Protocols

This section extensively discusses the review of the different IoT routing protocolsfor the secure routing in the IoT network.The routing protocol's main function is to find the best route between the sensors and sink nodes and then transmit the data. Routing always needs to choose best or shortestpath to reach the destination, and it needs to make use ofprotocols to accomplish source to destination.Communication can obtain by using either intradomain network or interdomain network . In IoT, the devices are mainly interacting with each otherfrom source to target devices which will process, store andanalysis the information. Efficient protocols must supportfor transmitting the data between the devices concerning lowenergy consumption and scalability .

In IoT, routing protocols classified into three types based upon wireless communications and given in Fig.1

1.Route Discovery
2.Network Organization
3.Protocol Operation.

3.1 Route Discovery

Route discovery refers to the process of finding a valid path or route between two or more nodes (devices) in a network, so that data can be efficiently and reliably transmitted from the source to the destination. This process is especially critical in packet-switched networks, such as the Internet, where data is divided into small packets and sent independently across the network. The primary goal of route discovery is to determine the most suitable path for data to travel, taking into account various factors such as distance, network congestion, link quality, reliability, and other performance metrics. Several routing algorithms and protocols have been developed to facilitate route discovery and enable efficient communication within networks. It consists of a reactive routing protocol, proactive routing protocol and hybrid routing protocol

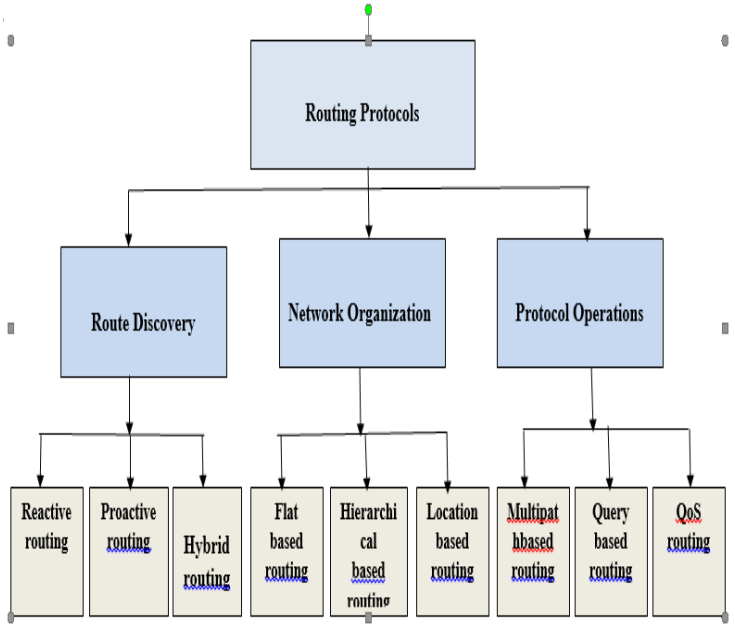

Fig:2Classification of Routing Protocols

3.1.1 Reactive routing protocol

Reactive protocols[34], the compute route take place and do not keep up the information of all nodes of network.on the other hand, do not maintain pre-established routes in routing tables. Instead, they initiate route discovery only when a node needs to send data to a destination for which it has no routing information. This on-demand nature reduces overhead in dynamic and large networks but can introduce additional delay during route discovery. Reactive routing protocols are based on Distance Vector concept (DV)[33] which can significantly decrease the routing overhead and the

https://doi.org/10.36282/IJASRM/8.9.2023.1902

power consumption. These protocols do not need to keep searching and maintaining the routes because there is no data traffic to send

Ad hoc On-Demand Distance Vector (AODV): AODV is a popular route discovery-based routing protocol used in mobile ad hoc networks. It operates on a reactive approach, where a node initiates a route discovery process only when it needs to send data to a destination for which it has no route information. The protocol then floods the network with route request packets to discover a path to the destination. Intermediate nodes cooperate in the process by forwarding the route request packets, and once the destination is reached or an existing route is discovered, a route reply packet is sent back to the source node, establishing the route. In AODV[35], Loop Free issue will be resolve by adding the sequence numbers in destination.AODV consists of three different message types. Route discovery will be performed by Route Request. Final routes will be decided by Route Replies. Link breakage error messages are warned by Route Errors in an active route in a network. A routing table should be maintained in AODV to keep all the information about the routes even if they are short lived routes.

The route discovery process involves broadcasting RREQ messages. These messages are propagated from node to node, seeking the destination node or an intermediate node with a valid route to the destination. Once a valid route is found, the destination node or the intermediate node storing the route sends a Route Reply (RREP) message back to the source node, establishing the route. Intermediate nodes update their routing tables to reflect the newly established route. Routes in AODV have a finite lifetime. If a route is not used for a certain period, it is considered expired, and its entry is removed from the routing tables. This mechanism helps keep the routing information up-to-date and relevant. AODV includes mechanisms to prevent routing loops during the route discovery process, ensuring that the selected route is loop-free.

TORA: Temporarily ordered routing algorithm [57] be an on-demand routing protocol. The purpose of TORA is to restrict the control message. TORA use the algorithm called link reversal. The TORA is a reactive routing type that was developed to address the challenges of ad hoc networks. TORA is unique in that it a distributed algorithm to maintain database of nodes and their connections, allowing for efficient route creation maintenance in a dynamic environment. TORA organizes nodes into multiple levels (such as the Ground, Mid, and Top levels). Each level manages different aspects of the routing process, which allows for more efficient and localized route updates. When a node wants to communicate with another node and no valid route exists, TORA initiates a route discovery process. The route is then established from the source to the destination node through a series of control messages. TORA uses temporal ordering to ensure that control messages are processed in a specific sequence, avoiding inconsistencies and potential routing loops during route creation and maintenance. TORA minimizes the control message overhead by maintaining routing information locally. Each node is responsible for updating its neighboring nodes about changes in its own state, helping to reduce network-wide broadcasting of control messages.

DSR: Dynamic Source Routing, is a reactive routing protocol used in mobile ad hoc networks (MANETs). DSR is designed to provide efficient and loop-free routing in highly dynamic and self-configuring wireless networks. When a source node wants to send data to a destination node and does not have a valid route, it initiates a route discovery process. The source node broadcasts a Route Request (RREQ) packet throughout the network. The RREQ contains the source and destination addresses, as well as a unique sequence number to avoid loop formation.

Intermediate nodes that receive the RREQ check their routing tables to determine if they have a valid route to the destination or have seen the destination before. If a node has a valid route, it creates a Route Reply (RREP) packet, which is unicast back to the source node.

The RREP contains the complete route from the source to the destination, which is stored at the source for future use.DSR is based on source routing, which means that the entire route from the source to the destination is included in the data packets. Each intermediate node forwards the packet based on the pre-calculated route, which eliminates the need for intermediate nodes to maintain routing tables.Nodes in DSR cache the route information obtained during the route discovery process. If the same route is needed again, it can be reused from the cache, reducing the overhead of subsequent route discoveries.DSR includes mechanisms for route maintenance. If a link in the established route breaks or if a node moves out of range, route error messages (Route Error - RERR) are sent back to the source node. Upon receiving RERR messages, the source node can initiate a new route discovery process to find an alternative route.

3.1.2 Proactive routing protocols :It also known as table-driven or proactive link-state routing protocols, maintain up-to-date routing information for all nodes in the network continuously. These protocols work well in stable and well-connected networks, where the topology changes are relatively infrequent. This proactive protocol maintains information in a tabular format which can be called as a routing table.

Optimized Link State Routing (OLSR): It is a proactive routing protocol designed specifically for mobile ad hoc networks (MANETs). OLSR aims to optimize the efficiency of link state routing in dynamic and self-configuring wireless networks. To maintain a proper topology of the network at each and every node, it involves in exchanging messages periodically. One of the primary innovations in OLSR is the use of Multipoint Relays (MPRs) to reduce the flooding of control messages. MPRs are selected nodes that efficiently forward control messages to their one-hop neighbors. By selecting a subset of nodes as MPRs, OLSR reduces the overhead associated with flooding, which is common in traditional link-state protocols.

MultiPoint Relay Selector algorithm in OLSR determines the nodes that will serve as MPRs. MPRS nodes

https://doi.org/10.36282/IJASRM/8.9.2023.1902

are those that have a large number of one-hop neighbors and cover a significant portion of the network, ensuring efficient message propagation. OLSR includes a proactive mechanism for controlling the network topology. Nodes periodically broadcast HELLO messages to inform their neighbors of their presence. Based on these HELLO messages, each node can construct a neighbor set, and the MPRS algorithm is used to select MPRs from this set. Optimized Path Calculation calculates routes based on the up-to-date link state information present in the network. With the use of MPRs, the control message overhead is reduced, leading to faster and more efficient route calculations.OLSR is designed to support nodes with multiple network interfaces .It can handle the complexity of managing multiple interfaces while maintaining efficient routing.

Destination-Sequenced Distance Vector(DSDV):

It is a proactive distance-vector routing protocol used in mobile ad hoc networks (MANETs). DSDV is based on the classic distance-vector algorithm but includes some enhancements to handle the challenges posed by the dynamic nature of mobile networks. In DSDV, each entry in a node's routing table contains a sequence number. The sequence number is assigned by the destination node and is used to identify the most recent routing information. This helps to avoid the "count-to-infinity" problem that can occur in traditional distance-vector protocols when network topology changes.

DSDV nodes exchange routing updates at regular intervals to ensure that all nodes have consistent and up-to-date routing information. These updates are broadcast throughout the network, allowing nodes to maintain accurate routing tables. DSDV uses the split horizon technique to prevent the propagation of incorrect routing information. Additionally, it employs the "poison reverse" mechanism, which advertises an infinite metric (usually hop count) for routes that have been invalidated. This helps in faster convergence when routes are broken or changed.When a node detects a change in its routing table (due to link failure or new route availability), it advertises the changes to its neighboring nodes during the periodic updates. The neighboring nodes, in turn, propagate the changes further in the network.By using the sequence numbers and split horizon with poison reverse, DSDV ensures that routes are loop-free, avoiding routing loops that can occur in distance-vector protocols.

3.1.3 Hybrid Routing Protocols: Hybrid protocols combine elements of both proactive and reactive approaches, offering a balance between real-time responsiveness and control overhead reduction. Examples: LOAD (Location Aided On-demand Routing), ZRP (Zone Routing Protocol).Hybrid protocols maintain proactive (continuous) and reactive (on-demand) routing components simultaneously. Proactive components establish and update routes continuously, while reactive components initiate route discovery only when needed. Hybrid protocols can dynamically adjust their behavior based on network conditions. When the network is relatively stable, proactive mechanisms help maintain up-to-date routes, reducing the delay in data transmission. In contrast, during topology changes or route failures, reactive mechanisms are activated to find alternative paths. By combining proactive and reactive approaches, hybrid protocols can optimize control message overhead. Proactive mechanisms help distribute routing information efficiently, while reactive mechanisms reduce unnecessary control message flooding. The proactive component of hybrid protocols ensures that the most common routes are readily available in the routing tables, reducing the time needed to establish data paths. In dynamic scenarios, the reactive component can quickly find alternative routes when topology changes occur.

ZRP: ZRP [36] is an hybrid protocol designed for mobile ad hoc networks (MANETs) to provide efficient and scalable routing in dynamic and large-scale networks. The main use of ZRP is data transmission is very fast and minimizes the overhead. ZRP wont transmission to entire network. Zone radius will specify the distances between the nodes. In ZRP, the network is divided into zones. Each node is a member of at least one zone, and some nodes, known as zone border nodes, may belong to multiple zones. Zone divisions help reduce the control message overhead by limiting the scope of routing updates to a specific zone.

In Intra-zone zone, a proactive routing protocol is used to maintain routing information among the nodes. Typically, a distance-vector or link-state routing protocol is employed. This proactive mechanism ensures that nodes have up-to-date routes to destinations within their respective zones. In inter-zone , When a node wants to communicate with a destination that is outside its zone, ZRP employs reactive routing. The node initiates a route discovery process using a reactive protocol such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing). The route discovery is limited to the nodes within the source node's zone, which helps in reducing control message overhead .Border casting is a technique used in ZRP for efficient inter-zone communication. When a node in one zone needs to broadcast a message to nodes in a neighboring zone, it forwards the message only to the zone border nodes that are part of both zones. This reduces the number of messages forwarded between zones.ZRP includes mechanisms to maintain routes, both proactive and reactive. Proactive routes are updated periodically, and reactive routes are invalidated or updated based on changes in the network topology.

3.2 Network Organization

Network organization refers to the way nodes in a network are structured and interconnected to facilitate the exchange of routing information and data packets. The network organization plays a crucial role in determining how routing decisions are made and how efficiently and reliably data is transmitted between nodes. Routing protocols can be categorized into be flat based, hierarchical, or location based, depending on the network architecture.

3.2.1 Flat-based routing:

https://doi.org/10.36282/IJASRM/8.9.2023.1902

The flat routing, also known as data-centric routing, the routes are formed in such regions that have data to transmit.Data-Centric Protocols are a class of routing protocols used in Wireless Sensor Networks (WSNs) that focus on efficient data-centric communication. These protocols are designed to optimize data dissemination and aggregation, making data the primary interest rather than individual sensor nodes. Data-Centric Protocols aim to reduce redundancy in data transmission, conserve energy, and enhance network scalability. Flat-based routing[35] is a contention-based scheduling. In IoT, this network is used to give a suitable a solution for many independent problems which occur due to their low operational complexity and high efficiency. This Flat-based routing is again classified into different types there are SPIN, Directed Diffusion, Rumor Routing, MCFA,Gradient-based routing

Sensor Protocol for Information via Negotiation (SPIN): SPIN is a communication protocol designed for wireless sensor networks (WSNs). It is a distributed and adaptive protocol that focuses on energy efficiency, reducing communication overhead, and prolonging the network's lifetime. SPIN uses data-centric communication, where messages are organized around data attributes rather than explicit node addresses. This approach allows nodes to express their data requirements and share information efficiently, reducing the number of control messages needed for communication. SPIN introduces a negotiation mechanism that enables nodes to request specific data from their neighbors. When a node requires certain information, it sends a request message to its neighbors, asking them to provide the desired data. Neigh boring nodes can then respond with the requested data if they have it, reducing unnecessary broadcasts and conserving energy.

SPIN's use of data-centric communication and negotiation-based information sharing contributes to energy efficiency in WSNs. By minimizing unnecessary communication and focusing on data of interest, SPIN reduces the amount of energy spent on message transmission and processing. As a result, the network's lifetime is extended, which is critical for battery-powered sensor nodes with limited energy resources.

Directed Diffusion (DD): Directed Diffusion is a data-centric communication paradigm and routing protocol designed for wireless sensor networks (WSNs). In direct diffusion(DD)[2], data generated by the nodes is represented by its <ATTRIBUTE • VALUE> tuple. The user's query is passed by the BS to each of the nodes in the WSN. The user's query travels all through and the same is compared with the event record stored in the node. If the event record matches with the query, then the data is sent to the BS otherwise the same query is passed onto its neighbouring nodes.Directed diffusion consists of several elements:

Interest Specification: Sensor nodes specify their data interests (attributes) and how they want to receive the data. Interests are defined as attributes and values, such as "temperature" with a desired range of values. Nodes express these interests through interest packets (called "interest" or "request" packets) periodically or based on events.

Data Dissemination: Nodes that generate data (source nodes) periodically transmit data packets, which include the data, attribute-value pairs, and a name that corresponds to the data's attributes. These data packets are diffused into the network without a predefined destination address.

Gradient-Based Communication: Upon receiving an interest packet, neighboring nodes create gradients (paths) towards the interest's source. The gradient contains information about the direction and quality of the path (e.g., signal strength). The gradients are used to guide data packets back to the interested nodes.

Data Collection: When data packets are transmitted into the network, they follow the gradients towards nodes that have expressed interest in the data. Intermediate nodes store data and aggregate it if multiple data packets are received for the same interest.

Reinforcement: Directed Diffusion uses a reinforcement mechanism to improve the quality of communication paths. Nodes can reinforce the gradients by sending interest packets more frequently or by caching data locally for future requests.

Rumor Routing (RR): The main idea behind Rumor Routing is to use probabilistic forwarding based on a "gossiping" or "rumor spreading" concept to disseminate data throughout the network.

In Rumor Routing, each node in the network maintains a table with entries for data items it has encountered. When a node generates new data or receives data from another node, it probabilistically forwards this data to its neighboring nodes. The forwarding decision is based on the data's popularity, which is determined by the number of times the data has been seen or forwarded by the node.

3.2.2 Hierarchical Routing Protocols [28] are a category of routing that organize the sensor nodes into a hierarchical structure to improve network efficiency, scalability, and energy consumption. In hierarchical WSNs, nodes are grouped into clusters, and each cluster has a designated cluster head responsible for data aggregation and communication with the base station or sink. Hierarchical Routing Protocols aim to reduce communication overhead, prolong network lifetime, and enhance network management. Clustering has the potential to reduce energy consumption and extend the lifetime of the network. Each cluster will have a cluster head that routes the information to the base station. Hierarchical routing decreases the complexity of network topology, increases routing efficiency, and causes much less congestion because of fewer routing advertisements. The main challenge is to reduce the overhead required to maintain the clusters. A large overhead can easily waste network resources. Overhead is reduced, which leads to a significant decrease in energy consumption.

Low-energy adaptive clustering hierarchy (LEACH): LEACH is a classic and widely used

https://doi.org/10.36282/IJASRM/8.9.2023.1902

clustering-based protocol for IoT-enabled WSNs. It forms a hierarchical network with cluster heads rotating among nodes to distribute energy consumption. It is a progressive, self-organizing protocol that chooses cluster heads in a rotation manner randomly over time. . The LEACH protocol decreased the energy consumption in WSNs. Sensor nodes communicate directly with their respective cluster head, reducing long-distance transmissions and saving energy. LEACH-based routing protocols are classified into into CH selection, data transmission, and both CH selection and data transmission techniques. The hierarchical structural design of a cluster-based can be set up by using distributed algorithm or centralized algorithm [45].

Liang, H et. Al. [42] worked on reducing energy consumption during data routing using LEACH and increasing the network life cycle. The number of optimal cluster representatives was estimated according to the overall energy lost for each round to decrease overhead due to excess selection of cluster monitors. A Voronoi diagram was used to select cluster nodes nearer to optimal cluster heads. Therefore, communication in the intra-cluster reduced energy consumption. The improved LEACH called improved chain-based clustering hierarchical routing (ICCHR) was periodic and partitioned into two stages per round i.e. formation of cluster regions and stability to data communication [46].

Threshold-sensitive Energy Efficient sensor Network protocol(TEEN): TEEN is a hierarchical clustering protocol, which groups sensors into clusters with each led by a CH[50]. It is a protocol that has been used in wireless sensor networks to optimize energy consumption and prolong the lifespan of the sensor nodes. TEEN is designed to be energy-efficient, making it suitable for applications where sensors are deployed in remote or hard-to-reach locations with limited power resources. TEEN is an enhancement of LEACH that introduces a threshold mechanism to trigger data transmission. Nodes only send data to the base station if the sensed values exceed a predefined threshold, reducing unnecessary data transmissions and conserving energy. The basic idea behind TEEN is to introduce a threshold-based mechanism for data transmission. Instead of transmitting data continuously or at fixed intervals, sensors in the network only send information when certain predefined thresholds are met or exceeded. This approach minimizes unnecessary communication and reduces energy consumption, as data is transmitted only when it is considered significant or meets specific criteria. TEEN employs three main components in its operation:

Event Detection: The sensor nodes continuously monitor the environment for events or changes in the data they are sensing. These events can be related to temperature, humidity, motion, light, or any other parameter of interest.

Thresholding: TEEN uses predefined threshold values for each sensor parameter. When a sensor detects an event that surpasses its set threshold, it triggers the data transmission process.

Data Transmission: Once an event is detected and its threshold is crossed, the sensor node transmits the relevant data to the base station or the sink node in the network. The base station can then process, analyze, and act upon the received data.

Power-Efficient Gathering in Sensor Information Systems(PEGASIS): PEGASIS is a hierarchical clustering-based routing protocol designed for wireless sensor networks (WSNs) and it was proposed as an improvement over traditional flat routing protocols in order to increase the network's energy efficiency and prolong the overall network lifetime.PEGASIS forms a chain-based network, where nodes transmit data to the nearest neighbor in the chain, and data is forwarded towards the base station through the chain. The main characteristic of a chain is that every node transmits data only to the two nearby neighbor nodes and only one sensor node can be selected to communicate with BS[51]. Collected data are transferred from node to node being aggregated and finally transmitted to the BS.It reduces the energy expenditure on long-distance transmissions and provides scalability.

In a wireless sensor network, sensor nodes are often densely deployed and have limited energy resources. Therefore, efficient utilization of energy becomes a critical factor in designing protocols for such networks. PEGASIS aims to minimize the energy consumption during data transmission and prolong the network's operational life time.The key idea behind PEGASIS is to organize the sensor nodes into a chain or a sequence, where each node acts as a relay for its neighboring nodes. The chain is formed in a way that the node closest to the base station (sink node) becomes the first node in the chain, and the node farthest from the sink node becomes the last node. The data gathered by each sensor node is then forwarded in a single-hop manner to the next node in the chain until it reaches the sink node.The protocol operates in a round-robin fashion, meaning that during each round, a different sensor node is chosen to be the leader of the chain. The leader is responsible for collecting data from its neighboring nodes and transmitting it to the sink node. The rotation of the leadership position helps balance the energy consumption across the network, as no single node consistently acts as the main relay.The advantages of PEGASIS include:

Energy Efficiency: By minimizing the distance data needs to travel and reducing the number of multi-hop transmissions, PEGASIS helps conserve energy and extend the network's lifetime.

Scalability: The hierarchical structure of the protocol makes it scalable, even for large sensor networks, as it avoids the overhead associated with maintaining routing tables.

Fault Tolerance: Since the data is transmitted in a single-hop manner, the failure of a single node does not affect the entire network's connectivity.

3.2.3 Location-Based Protocols:

Location-based routing is a type of routing technique used in wireless networks where the routing decisions are based on the physical locations or geographical coordinates of the network nodes. Instead of relying on traditional routing metrics like hop counts or network topology information, location-based routing protocols use the actual positions of the nodes to

https://doi.org/10.36282/IJASRM/8.9.2023.1902

determine the next hop for data transmission. They are located mostly by means of GPS. Location-based routing is particularly useful in scenarios where nodes are equipped with GPS (Global Positioning System) receivers or other location-aware technologies. This includes wireless ad hoc networks, mobile sensor networks, vehicular networks, and other applications where nodes have the ability to determine their own positions accurately. The distance between nodes is estimated by the signal strength received from those nodes and coordinates are calculated by exchanging information between neighboring nodes.

Location-based protocols often require less control and maintenance overhead compared to traditional routing protocols, as they don't rely on periodic flooding of routing information or the maintenance of complex routing tables.Improved Scalability: Since routing decisions are made based on location information, location-based protocols can scale well to large networks, as they don't depend on the knowledge of the entire network topology.Adaptability to Dynamic Location-based routing can adapt more easily to dynamic network conditions, such as node mobility or changes in the network topology, by continuously updating routing decisions based on real-time location updates. By using shorter and more direct communication paths, location-based routing can help reduce the energy consumption of individual nodes and extend the overall network lifetime.

Geographic adaptive fidelity (GAF) protocol: GAF is energy-aware routing protocol which was originally made for MANETs, but it can also apply to sensor networks. This protocol deactivates nodes that are less participating in the routing decisions in the network with no impact in the routing performance, and hence save energy in the network. GAF is based on mechanism of turning off unnecessary sensors while keeping a constant level of routing fidelity (or uninterrupted connectivity between communicating sensors).A Global Positioning System (GPS) sensor is attached to every node to indicate its location, which will enable the nodes to remember itself with a point on the virtual grid. In GAF, sensor field is divided into grid squares and every sensor uses its location information, which can be provided by GPS or other location systems. . GAF aims to maximize the network lifetime by reaching a state where each grid has only one active sensor based on sensor ranking rules. The ranking of sensors is based on their residual energy levels. Thus, a sensor with a higher rank will be able to handle routing within their corresponding grids. For example, a sensor in the active state has a higher rank than a sensor in the discovery state. A sensor with longer expected lifetime has a higher rank.

Geographic and energy aware routing (GEAR) protocol:GEAR protocol is a routing algorithm designed efficiently transmit data between nodes while considering both geographical information and energy constraints. GEAR is based on energy and location aware[53].WSNs are composed of small, low-power sensors that are distributed over a geographical area to monitor and collect data about the environment. Traditional routing protocols may not be suitable for WSNs due to their resource constraints, especially the limited energy supply of individual sensor nodes. GEAR protocol addresses these challenges by taking into account the spatial information of sensor nodes and their energy levels, thus optimizing the routing paths and prolonging the network's overall lifetime.

GEAR aims to conserve the energy of sensor nodes by selecting paths that minimize the energy consumption during data transmission. It achieves this by considering the remaining energy levels of nodes along potential routes.Unlike some other routing protocols that use abstract addressing or IDs, GEAR utilizes the physical location information of sensor nodes. This allows the protocol to take advantage of the spatial distribution of nodes to establish efficient communication paths.

GEAR strives to balance the energy consumption across the network by avoiding routes that pass through nodes with low energy levels. Instead, it selects paths that distribute the communication load more evenly.GEAR is designed to adapt to changes in the network topology, such as node failures or the addition of new nodes. It dynamically adjusts the routing paths based on the current state of the network. GEAR protocol combines geographic awareness and energy efficiency to enhance the performance and prolong the lifetime of wireless sensor networks. It's particularly suited for applications where energy conservation and spatial information are critical, such as environmental monitoring, surveillance, and industrial automation.

3.3 Protocol Operation

It gives a brief description of the main operational characteristics of routing protocols like communication pattern, hierarchy, delivering methods, computation.

3.3.1 Multipath-based Protocols: Multipath-based routing is a routing strategy that involves the use of multiple paths for transmitting data between source and destination nodes[34].It aims to improve network performance, reliability, and efficiency by distributing data traffic across multiple routes instead of relying on a single path. mproved Reliability: Using multiple paths reduces the impact of node failures or link disruptions on data delivery. If one path becomes unavailable, data can still be transmitted through alternative paths.Multipath routing helps to distribute traffic evenly across multiple paths, preventing congestion on a single route and optimizing network utilization.By splitting data traffic across multiple paths, the network's overall throughput capacity can be increased.Data can reach its destination more quickly through parallel transmission along multiple paths.Distributing data transmission across multiple paths can help balance energy consumption among nodes, potentially extending the network's overall lifetime. MORE and MMSPEED are the multipath routing protocol

Path Discovery: The process of identifying multiple available paths between the source and destination nodes. This can involve various mechanisms like proactive path establishment or on-demand path discovery.

Path Selection: After discovering multiple paths, the routing protocol selects the most suitable paths based on

https://doi.org/10.36282/IJASRM/8.9.2023.1902

specific metrics such as path length, link quality, residual energy of nodes, and load distribution.

Packet Duplication: Data packets are duplicated and sent through the selected paths simultaneously. Each duplicate contains information to indicate the intended destination.

Packet Forwarding: Intermediate nodes along the paths receive duplicated packets and forward them toward the destination. This process ensures that data packets reach their destination using redundant paths.

Packet Aggregation: Some multipath protocols incorporate packet aggregation, where intermediate nodes aggregate duplicated packets to reduce redundancy and conserve energy before forwarding them.

Packet Reordering and Reconstruction: At the destination, received packets from different paths may arrive in different orders. The destination node needs to reorder and reconstruct the original data stream.

Path Maintenance: Multipath routing protocols must continuously monitor the quality and reliability of each path. If a path becomes unreliable or congested, the protocol might reroute the traffic or deactivate the problematic path.

MORE (Multipath Opportunistic Routing): A protocol that uses multiple paths to increase the likelihood of successful packet delivery, especially in dynamic and unpredictable environments.

MMSPEED (Multipath Multi-SPEED): A protocol that provides both single-path and multipath routing options, allowing nodes to choose between them based on network conditions.

3.3.2 Query-based routing: Query-based routing is a type of routing strategy where communication paths are established and data is transmitted in response to specific queries or requests. This approach allows nodes in the network to selectively gather and transmit data relevant to certain queries, optimizing energy usage and minimizing unnecessary data transmissions. A query-based routing protocol intended to consider both vitality and separation while directing bundles over a system[54].

A node, often referred to as a "query originator" or "query generator," initiates a query by sending a request for specific information to the network. The query specifies the type of data and the criteria for selection.The query is propagated through the network using a routing protocol. Nodes that receive the query evaluate whether they have the requested data or information that matches the query's criteria.Nodes that have the requested data or can generate the required information in response to the query prepare to transmit it back to the query originator.The routing protocol determines the paths for transmitting data back to the query originator. These paths might involve a combination of unicast, multicast, or even multipath routing, depending on the network topology and requirements.Nodes with relevant data transmit their responses or data packets back to the query originator along the selected paths.Intermediate nodes or query processing nodes may aggregate, filter, or process the data before forwarding it toward the query originator. This can help reduce redundancy and save energy.Once the query originator receives the responses or data, the query is considered fulfilled, and the process concludes.

Advantages of Query-Based Routing:

Energy Efficiency: Since data transmission is initiated based on specific queries, unnecessary data transmissions are minimized, leading to energy savings in resource-constrained WSNs.

Selective Data Gathering: Query-based routing allows the network to focus on collecting and transmitting only the data that is relevant to the specific queries, optimizing data usage

Reduced Overhead: The protocol overhead associated with broadcasting data to all nodes is reduced, leading to better network scalability

Dynamic Data Collection: The network can adapt to changing data needs by generating new queries, allowing nodes to gather real-time or recent information as required

3.3.3 QoS routing protocols: Quality of Service (QoS) routing protocols aims to optimize data transmission by considering various QoS metrics such as reliability, latency, energy efficiency, and bandwidth utilization. These protocols ensure that data is delivered according to specific application requirements. The ACQUIRE and MMSPEED are kind of protocols, which worked on QoS routing protocols.

Adaptive Quality of service Controlled, energy-Aware, and Interference-REsponsive Routing(ACQUIRE): It is a routing protocol that considers energy efficiency and interference management while delivering QoS in WSNs. It adapts to changing network conditions and can reroute data to avoid interference and ensure reliable and timely delivery of packets. It is adaptive, meaning it can respond to changing network conditions. This adaptability is crucial in WSNs, where network topology, energy levels, and interference can vary over time. It is designed to conserve the energy of sensor nodes, which is a critical concern in WSNs due to the limited energy resources of these devices. It achieves this by optimizing routing decisions to minimize energy consumption.

MultiSink Multi-SPEED (MMSPEED): It is designed for multimedia applications in WSNs. It focuses on providing QoS for real-time video and audio streaming by considering factors like packet loss, delay, and jitter. It optimizes routing paths to meet the QoS requirements of multimedia data. It is specifically designed for multicast communication, where data needs to be transmitted from one sender to multiple receivers efficiently. This is particularly relevant for multimedia applications where multiple sensor nodes may need to receive the same data stream.It takes into account the limited energy resources of sensor nodes. It employs energy-efficient routing strategies to reduce energy consumption during data transmission, helping to prolong the network's lifetime

https://doi.org/10.36282/IJASRM/8.9.2023.1902

International Journal of Advanced Scientific Research and Management, Volume 7 Issue 9, Sept 2023

IJASRM

www.ijasrm.com

ISSN 2455-6378

Literature Review on Secure and Energy Efficient Routing protocols

This section presents the surveys performed on linking the need for lifetime extension with respect to applications of WSN are presented to show how energy consumption is essential according to application type

Lucia Keleadile Ketshabetswe et. al. [56] focused on different solutions to improve network lifetime and surveyed energy efficient routing protocols. Along with network modeling, the paper presented event extraction analysis and differentiated RPs based on homogeneous and heterogeneous routing protocols. Further, they sub-classified them concerning static, mobile, and other aspects. Lastly, they compared the performance of a few routing protocols and suggested future work directions to be considered. Some of the factors listed for designing WSN and routing protocols were energy capacity,non-static networks, node placement,

Pantazis et al. [31] presented routing methods for WSNs and their related protocols have been analysed here. Protocol like SPIN, LEACH, DECA, HEED and PEGASIS are considered as energy efficient than their previous models. Main problems with these protocols are that networks are supposed to be static and nodes are assumed as stationary. This work reviewed various types of the routing protocols which all save energy and increase lifespan of sensor network by saving energy of sensor nodes by using various techniques. Authors have reviewed and evaluated diverse proposed models, processes, set of rules, and applications. Based on this survey it is concluded that there are many more existing issues which may be addressed and to be solved in context on WSN applications, communication architectures, information security, and power management. They provide a detailed comparison among these protocols in terms of network scalability, nodes mobility, power usage, route selection metrics, periodic message type, and robustness. They also classified the protocols according to duty-cycling, data driven and mobility to prove that the energy consumption of the radio is much higher than the energy consumption due to data sampling or data processing.

Trupti Mayee Behera et al[38] proposed a brief description of LEACH-based and bio-inspired protocols, their advantages and disadvantages , assumptions, and the criteria of CH selection. The performance factors such as scalability, and packet delivery ratio of various protocols are compared. The classification of routing protocols is performed based on a homogenous and heterogeneous environment suitable for the specific application has been discussed.A homogeneous WSN consists of nodes with the same initial energy, and a heterogeneous sensor network contains nodes of two or more energy levels. various approaches to prolong network lifetime in WSNs is considered because sensors become inaccessible after deployment. The design challenges for routing protocols in WSNs are outlined. Numerous clustering strategies are highlighted, which are projected with comprehensive routing techniques, resulting in improved performance

Mohamed, Reem E. [60] have classified the WSN-based applications on various aspects in order to indicate the main sensor position, fault resistance, latency, information aggregation, and scalability.

Khalil et. al [57] listed out the importance of routing protocol for smart cities and reviewed them for productive research and proposed how their classification can be useful for operational utility. They segregated the routing techniques based on operation and utility and classified them concerning four parameters including topology, data-centric, location assisted, and mobility-based. Lastly, they discussed the requirement of the reviewed routing technique in dominant areas.

Khan et al. [58] presented a high-level taxonomy of energy management in WSNs. They categorized energy provision approaches as battery driven, energy harvesting, and energy transference based schemes. They recommend considering both, the energy supply as well as the energy consumption in parallel while designing an energy efficient algorithm

issues related to protocol design. Hence, the efficiency of the energy in the recent proactive routing protocols is investigated from various aspects. The energy fairness and energy overhead in each protocol were analyzed. The most energy-efficient routing protocols for homogeneous proactive networks were investigated and they were compared. The Wireless Sensor Network (WSN) energy efficiency results from three fundamental necessities: network overhead within network arrangement and re-arrangement, selecting a route for data transmission, and fault tolerance or network adaptability.The significance of routing protocol algorithms, existing challenges, and future trends in routing in IoT are described efficiency.

Rani et al. [61] proposed an improved solution for organizing objects to implement an energy-efficient and scalable IoT. Firstly, the framework was presented to deploy the IoT with scalability features providing higher extensibility. Afterward, considering the framework, an optimization outline can support the deployment of an IoT with energy efficiency. This optimization outline is confined by the loads on wireless links and energy expenses. Compared to conventional WSN outlines in terms of network lifetime, time, and scalability, various numerical tests confirm superiority of the proposed outline.

Shen et al. [62] presented an energy-efficient centroid-based routing protocol (EECRP) for controlling the WSN-assisted IoT energy. An enhancement algorithm was presented regarding the number of cluster head nodes and the number of dead nodes. The simulation results indicated that with the base station (BS) deployment in the network, it would be possible to transfer a great amount of data by the EECRP with very low energy dissipation. The EECRP has a longer network lifetime than the GEEC, LEACH-C, and LEACH.

Sang-Hyun Park et al. [63] designed an Energy-Efficient Probabilistic Routing (EEPR) algorithm for controlling the routing request packets transmission. EEPR enhanced the network lifetime, while minimizing the Packet Loss Ratio (PLR). The probabilistic control was made by utilizing the Expected Transmission Count (ETX) metric in the AODV protocol context and node's residual energy. The results revealed that the EEPR algorithm provided better network

https://doi.org/10.36282/IJASRM/8.9.2023.1902

lifetime along with even consumption of node's residual energy.

Greg Kuperman et al. [64] made research on the importance of the routing protocols in the efficient and reliable data communication in the multi-hop wireless network of the IoT environment. The link-based routing leads to the PLR, high maintenance cost, and unreliable data transmission within the network. The unfit nature of the link-based routing protocols for the wireless networks was explored in this research by comparing the performance of AODV and Optimized Link State Routing (OLSR) in terms of mobility, Routing Success Probability (RSP), the distance between users, PDR and overhead.

Conclusion

One of the main challenges in the design of routing protocols for WSNs is energy efficiency due to the scarce energy resources of sensors. The ultimate objective behind the routing protocol design is to keep the sensors operating for as long as possible, thus extending the network lifetime. routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors.This review aims to comprehensively analyze and compare different routing protocols used in Wireless Sensor Networks for IoT applications. The comparative analysis will highlight the trade-offs between different protocols and their suitability for specific IoT application scenarios.. In the context of IoT applications, where real-time data exchange and intelligent decision-making are paramount, the effectiveness of routing protocols becomes a key determinant of the overall system performance. Accordingly, energy efficient routing protocols should be carefully chosen according to system requirements and application needs.

References

[1] N.A. Pantazis, S.A. Nikolidakis, D.D. Vergados, Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey, IEEE Commun. Survey. Tutorials (2013).

[2] Ravi Kishore Kodali, Prof. Narasimha Sarma, "Energy Efficient Routing Protocols for WSN's", International Conference on Computer Communication and Informatics,2013

[3] Ashish Christian and Himanshu Soni, "Lifetime Prolonging in Leach Protocol For Wireless Sensor Networks," in International Conference On Intelligent Systems And Signal Processing, 2013.

[4] W. Guo and W. Zhang, "A survey on intelligent routing protocols in wireless sensor networks," J. Netw. Comput. Appl., vol. 38, pp.185–201, 2014.

[5] B Pithva, K Pattani and A Christian, "Optimization of Leach Protocol in Wireless Sensor Network," International Journal of Computer Applications, 2014.

[6] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ''Internet of things: A survey on enabling technologies, protocols and applications," IEEE Commun. Surv. Tut., vol. PP, no. 99, 2015.

[7] Alekha Kumar Mishra et al.,, "An Enhancement of PEGASIS Protocol with Improved Network Lifetime for Wireless Sensor Networks," in IEEE Power, Communication and Information Technology Conference, 2015.

[8] Mr. Tushar Chauhan, Ms. Meenakshi Nayyer," A Technical Review on Energy Efficient Protocol based on PEGASIS and LEACH", in International Journal on Recent and Innovation Trends in Computing and Communication(2016)

[9] Verdiere, Axel, et al. ''The Lightweight On-demand Ad hoc Distance-vector Routing Protocol-Next Generation (LOADng)." (2016).

[10] Zhao, Ming, Ivan Wang-Hei Ho, and Peter Han Joo Chong. ''An energy-efficient region-based RPL routing protocol for low-power and lossy networks." IEEE Int. Things J. 3.6 ,:1319- 1333,2016

[11] M. Fouladlou, A. Khademzadeh, An energy efficient clustering algorithm for Wireless Sensor devices in Internet of Things, Artif. Intell. Robot. (IRANOPEN).IEEE (2017).

[12] S. Sankar, P. Srinivasan, Composite metric based energy efficient routing protocol for internet of things, Int. J. Intell. Eng. Syst. 10 (5) (2017) 278–286.

[13] H.P. Alahari, S.B. Yalavarthi, A survey on network routing protocols in internet of things (IoT), Int. J. Comput. Appl. 160.2 (2017) 18–22.

[14] Waleed Ejaz et al., Efficient energy management for the internet of things in smart cities, IEEE Commun. Mag. 55.1 (2017) 84–91.

[15] Trupti Mayee Behera , Umesh Chandra Sama , Sushanta Kumar Mohapatra," Energy-efficient modified LEACH protocol for IoT application", IET Wireless Sensor Systems,2018

[16] .Vinod Kumar and Ajay khunteta, "Energy Efficient PEGASIS Routing Protocol for Wireless Sensor Networks," in 2nd International Conference on Micro-Electronics and Telecomm. Engineering, 2018.

[17] S.B. Shah et al., Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks, Fut. Gener. Comput. Syst. 81 (2018) 372–381.

[18] V. Saranya, S. Shankar, and G. R. Kanagachidambaresan, "Energy efficient clustering scheme (EECS) for wireless sensor network with mobile sink," Wirel. Pers. Commun., vol. 100, no. 4, pp. 1553–1567, 2018.

[19] A Hussein and R A Khalid, "Improvements of PEGASIS Routing Protocol in WSN," International Journal of Engg. Research, 2019.

[20] Adeeb Saaidah et al., An Efficient Design of RPL Objective Function for Routing in Internet of Things using Fuzzy Logic, Int. J. Adv. Comput. Sci. Appl. (IJACSA) (2019).

https://doi.org/10.36282/IJASRM/8.9.2023.1902

[21] Fadi Al-Turjman, Cognitive routing protocol for disaster-inspired internet of things, Future Gene. Comput. Syst. 92 (2019) 1103–1115.

[22] El Alami, H., Najid, A.: Optimization of energy efficiency in wireless sensor networks and Internet of Things: a review of related works. In: Nature-Inspired Computing Applications in Advanced Communication Networks, pp. 89–127, 2020.

[23] Vivek Sharma and Devershi Pallavi Bhatt ,"A Review on Recent Trends in Secure and Energy Efficient Routing Approaches in Wireless Sensor Networks" in IOP Conference Series: Materials Science and Engineering 2020

[24] Mohammed Réda El Ouadi, Abderrahim Hasbi, "Comparison of LEACH and PEGASIS Hierarchical Routing Protocols in WSN ",International Journal of Online and Biomedical Engineering .(2020)

[25] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network: optimized cluster head selection model.," Telecommun. Syst.,vol. 74, no. 3, 2020.

[26] .A. Aziz, K. Singh, W. Osamy, and A. M. Khedr, "An Efficient Compressive Sensing Routing Scheme for Internet of Things Based Wireless Sensor Networks," Wirel. Pers. Commun., vol. 114, no. 3, pp. 1905–1925, 2020.

[27] R. Manchanda and K. Sharma, "Energy efficient compression sensing-based clustering framework for IoT-based heterogeneous WSN.," Telecommun. Syst., vol. 74, no. 3, 2020.

[28] Malay Chakraborty , Surya Shekhar , Mrutyunjay RoutA "Comparative Analysis of LEACH and PEGASIS Hierarchical Protocol for Wireless Sensor Networks" in A Collection of Contemporary Research Articles in Electronics, Communication and Computation,2021

[29] Ban Ayad Ahmmad, Salah Abdulghani Alabady, "Energy efficient routing protocol developed for internet of things Networks", IET Quantum Communication,2022

[30] Ban Ayad Ahmmad, Salah Abdulghani Alabady, " Energy-efficient routing protocol developed for internet of things networks" - IET Quantum Communication(2023)

[31] Pantazis, N. A., Nikolidakis, S. A., Vergados, D. D., & Member, S. (2013). Energy-efficient routing protocols in wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 15(2), 551–591 doi:10.1109/surv.2012.062612.00084

[32] G. Jianlin, P. Orlik, Z. Jinyun, and K. Ishibashi. "Reliable routing in large scale wireless sensor networks". in Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on.2014. p. 99-104.

[33] Meeta Singh, Sudeep Kumar, "A Survey: Ad-hoc on Demand Distance Vector (AODV) Protocol ", in International Journal of Computer Applications (0975 – 8887), 2017

[34] Kaebeh Yaeghoobi S.B., M.K. Soni, S.S. Tyagi , " A Survey Analysis of Routing Protocols in Wireless Sensor Networks", in International Journal of Engineering and Technology,2015

[35] Ravi Kumar Poluru and Shaik Naseera ,"A Literature Review on Routing Strategy in the Internet of Things" in Journal Of Engineering Science and Technology ,2017

[36] Namrata Mahakalka, Rahul Pethe,"Review of Routing Protocol in a Wireless Sensor Network for an IOT Application", Proceedings of the International Conference on Communication and Electronics Systems (ICCES 2018)

[37] Amira Zrelli, "Hardware, Software Platforms, Operating Systems and Routing Protocols for Internet of Things Applications", Wireless Personal Communications,2021

[38] Trupti Mayee Behera et al,"Energy-Efficient Routing Protocols for Wireless Sensor Networks: Architectures, Strategies, and Performance", Electronics ,2022

[39] H.M. Aldosari, V. Snasel and A. Abraham, A New Security Layer for Improving the security of internet of things (IoT),International Journal of Computer Information Systems and Industrial Management Applications 8 (2016), 275-283.

[40] Sandeep Kaur , Supreet Kaur,"Analysis Of Zone Routing Protocol In Manet" IN International Journal of Research in Engineering and Technology,2013

[41] Murukesan Loganathan et al, "Energy efficient routing protocols for wireless sensor networks: comparison and future directions" in MATEC Web of Conferences,2017

[42] Liang, H., Yang, S., Li, L. et al. Research on routing optimization of WSNs based on improved LEACH protocol. J Wireless Com Network 2019, 194 (2019). https://doi.org/10.1186/s13638-019-1509-y

[43] Anamika Walter et al ,"Energy Efficient Routing Protocol In Wireless Sensor Network" International Journal of Computer Engineering and Technology (IJCET),2020

[44] Patel Bhoomika D, Patel Ashish D. "Hierarchical routing protocols in wireless sensor network" in Computer Technology & Applications,2015

[45] Manap, Zahariah, et al. "A review on hierarchical routing protocols for wireless sensor networks." Wireless personal communications 72.2 (2013): 1077-1104.

[46] Wu, H., Zhu, H., Zhang, L., & Song, Y. (2019). Energy Efficient Chain Based Routing Protocol for Orchard Wireless Sensor Network. Journal of Electrical Engineering & Technology, 14(5), 2137-2146.

[47] Daanoune, I.; Abdennaceur, B.; Ballouk, A. A comprehensive survey on LEACH-based clustering

https://doi.org/10.36282/IJASRM/8.9.2023.1902

routing protocols in Wireless Sensor Networks. Ad Hoc Netw. 2021, 114, 102409

[48] Priyanka M.Tambat and Arati M. Dixit, "Energy Efficient Scheme for Wireless Sensor Networks", International Journal on Recent and Innovation Trends in Computing and Communication,2015

[49] Hussein Mohammed Salman, "Survey of routing protocols in wireless sensor networks", International journal of sensors and sensor networks 2014

[50] Singh, Shio Kumar, M. P. Singh, and D. K. Singh. "Routing protocols in wireless sensor networks–A survey." International Journal of Computer Science & Engineering Survey (IJCSES) Vol 1 (2010): 63-83.

[51] Christos Nakas , Dionisis Kandris , and Georgios Visvardis " ,Energy Efficient Routing in Wireless Sensor Networks: A Comprehensive Survey", Multidisciplinary Digital Publishing Institute(MDPI),2020

[52] Y. X:u, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing", Proceedings ACM/IEEE MobiCom'01, Rome, Italy, July 2001, pp. 70-84.

[53] Y. Yu, R. Govindan, D. Estrin, Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks, Energy 463 (2001) 2–3, no. Report UCLA/CSD-TR-01-0023

[54] Swati Mishra et al , "A Literature Survey on Routing Protocol in Wireless Sensor Network", International Conference on Innovations in information Embedded and Communication Systems (ICIIECS),2017

[55] Uthra, R. Annie; Raja, S. V. Kasmir (2012). QoS routing in wireless sensor networks—a survey. ACM Computing Surveys, 45(1), 1–12. doi:10.1145/2379776.2379785

[56] Ketshabetswe, Lucia Keleadile, et al. "Communication protocols for wireless sensor networks: A survey and comparison." Heliyon 5.5 (2019): e01591.

[57] M Khalil, A Khalid, FU Khan and A Shabbir, "A Review of Routing Protocol Selection for Wireless Sensor Networks in Smart Cities", 24th Asia-Pacific Conference on Communications (APCC), IEEE, pp. 610-615, 2019.

[58] Khan, J. A., Qureshi, H. K., & Iqbal, A. (2016). Energy management in wireless sensor networks: A survey. Computers & Electrical Engineering, 41, 159–176.

[59] Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 11(9),2013–2027.doi:10.1109/tifs.2016.2570740

[60] Mohamed, Reem E., et al. "Survey on wireless sensor network applications and energy efficient routing protocols." Wireless Personal Communications 101.2 (2018): 1019-1055.

[61] Rani, S., Talwar, R., Malhotra, J., Ahmed, S.H., Sarkar, M. And Song, H., "A novel scheme for an energy efficient internet of things based on wireless sensor networks", Sensors, Vol. 15, No. 11, (2015), 28603-28626. https://doi.org/10.3390/s151128603

[62] Shen, J., Wang, A., Wang, C., Hung, P.C. and Lai, C.-F., "An efficient centroid-based routing protocol for energy management in wsn-assisted iot", Ieee Access, Vol. 5, (2017), 18469-18479.https://doi.org/10.1109/ACCESS.2017.2749606

[63] S-H. Park, S., Cho and J-R., Lee, Energy-efficient probabilistic routing algorithm for internet of things,Journal of Applied Mathematics (2014).

[64] G. Kuperman, S. Moore, B-N. Cheng and A. Narula-Tam, Characterizing deficiencies of path-based routing for wireless multi-hop networks, In Proceedings of the IEEE International Conference on Aerospace, USA (2017), 1-9

https://doi.org/10.36282/IJASRM/8.9.2023.1902