JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Investigation and Comprehensive Analysis On Routing For Internet Of Things (Iot) Networks

[1]S. Bharathi, [2]Dr. D. Maruthanayagam
[1]Research Scholar, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India
[2] Dean Cum Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.

Abstract: Routing plays a crucial role in facilitating communication and data exchange within Internet of Things (IoT) networks. This paper provides a comprehensive overview of routing techniques, protocols and strategies tailored for IoT deployments. The analysis begins with an introduction to the concept of IoT and highlights the importance of efficient routing in IoT networks. It discusses the fundamentals of routing in IoT, including the role of routing protocols in data transmission and the unique challenges posed by IoT environments**.** This revision explores various categories of routing protocols, including proactive, reactive, and hybrid protocols, and examines their characteristics, advantages, and limitations. Furthermore, the study reveals Quality of Service (QoS) routing in IoT, emphasizing the importance of delivering data with specific QoS requirements. QoS-aware routing protocols and mechanisms are examined to meet diverse QoS objectives and ensure satisfactory user experiences in IoT applications.

Keywords: Internet of Things (IoT), Routing Protocols, Quality of Service (QoS), Energy Efficiency, Security and Experimental Evaluation.

I.INTRODUCTION

The Internet of Things (IoT) refers to a network of interconnected devices, objects, or "things" embedded with sensors, software and other technologies to collect and exchange data over the internet or other communication networks. These connected devices can range from everyday objects such as household appliances, vehicles and wearable devices to industrial equipment, infrastructure systems and environmental sensors [1]. The core concept of IoT involves enabling these devices to communicate with each other autonomously, gather information from their surroundings through sensors and transmit data to centralized systems or other devices for processing, analysis and decision-making. This interconnectedness and data exchange among IoT devices enable the automation of various tasks, the monitoring of physical environments and the creation of new applications and services across a wide range of industries and domains. In essence, IoT enables the integration of physical objects into digital networks, allowing for seamless interaction between the physical and virtual worlds [2]. By connecting devices and collecting data from the physical environment, IoT enables organizations and individuals to gain insights, make informed decisions, improve efficiency, enhance safety and create innovative solutions to complex challenges.

1.1. Key components of IoT

The key components of the Internet of Things (IoT) encompass (cover) the fundamental elements that enable the seamless connectivity, data exchange and functionality within IoT systems [3] [4]. Figure 1 components include:

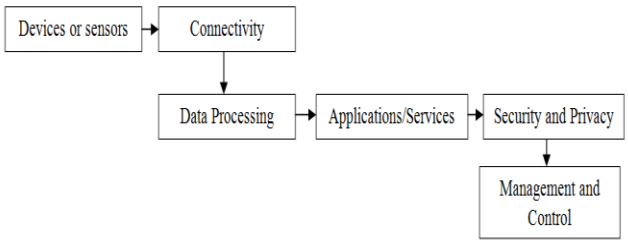

Figure 1: Key components of IoT

Devices/Sensors: Devices or sensors are the physical objects or things that form the foundation of the IoT ecosystem. These devices are equipped with sensors to collect various types of data from the environment or the objects they interact with. Sensors can measure a wide range of parameters such as temperature, humidity, light intensity, motion, pressure and more. Actuators are components that enable devices to perform actions based on the data collected, such as adjusting settings, activating alarms, or controlling other devices. Examples of IoT devices include smart thermostats, wearable fitness trackers, and industrial machinery with embedded sensors, smart appliances, and environmental monitoring systems.

Connectivity: Connectivity is essential for IoT devices to communicate with each other, with backend systems, and with users. IoT devices can connect to the internet or local networks using various communication technologies. Common connectivity technologies include Wi-Fi, Bluetooth,

Zigbee, Z-Wave, cellular networks (3G/4G/5G), Ethernet, and low-power wide-area networks (LPWAN) like LoRaWAN and NB-IoT. The choice of connectivity technology depends on factors such as range, data rate, power consumption, coverage area and cost. Different applications may require different connectivity solutions based on their specific requirements.

Data Processing: Data processing is a crucial component of IoT systems, where the collected data is analyzed to extract insights, detect patterns and make decisions. **Data processing involves collecting, storing, analyzing, and interpreting data generated by IoT devices**. Data processing can occur locally on devices (edge computing) or in centralized cloud-based systems. **Edge computing enables real-time data processing, reducing latency, bandwidth usage and reliance on cloud resources**. Cloud-based data processing offers scalability, storage capacity, and advanced analytics capabilities for processing large volumes of data. Data processing techniques include data filtering, aggregation, visualization, machine learning and predictive analytics. These techniques enable IoT systems to derive actionable insights, optimize operations, and support decision-making processes.

Applications/Services: IoT applications and services leverage the data generated by connected devices to deliver value-added functionalities and solutions across various domains. Examples of IoT applications include:

- ***Smart Home:*** Home automation systems for controlling lights, thermostats, security cameras and appliances.
- ***Industrial IoT (IIoT):*** Remote monitoring, predictive maintenance and asset tracking in manufacturing plants, oil refineries and utilities.
- ***Healthcare:*** Remote patient monitoring, wearable health trackers and smart medical devices for improving patient care and treatment outcomes.
- ***Smart Cities:*** Urban infrastructure management, traffic monitoring, waste management, and environmental monitoring to enhance sustainability and livability.

IoT services encompass software platforms, cloud services, analytics tools and applications developed to address specific use cases and industry needs.

Security and Privacy: Security and privacy are critical considerations in IoT deployments to protect sensitive data, **ensure device integrity and prevent unauthorized access or malicious attacks**. Key security measures for IoT systems include:

- ***Encryption:*** Securing data transmission and storage using cryptographic techniques to **prevent eavesdropping and tampering**.
- ***Authentication:*** Verifying the identity of users, devices and services to **prevent unauthorized access**.
- ***Access Control:*** Limiting privileges and enforcing permissions to **restrict access to resources** and functionalities.
- ***Regular Security Updates:*** Keeping devices and software up-to-date with the latest security patches and **fixes to address vulnerabilities**.

Privacy concerns in IoT relate to the collection, use and sharing of personal data by connected devices and services. Implementing privacy-by-design principles, transparent data practices and user consent mechanisms can help address these concerns and build trust among users.

Management and Control: IoT systems require management and control mechanisms to monitor device status, configure settings, perform updates and troubleshoot issues. Device management platforms enable remote device provisioning, configuration, monitoring, and firmware/software updates. **Control systems allow users or automated processes to interact with IoT devices**, set rules, trigger actions, and adjust settings based on predefined criteria.

1.2. Architecture of IoT

The architecture of IoT (Internet of Things) refers to the structure and components of an IoT system that enable the connection, communication, data processing and interaction between IoT devices, networks and applications. **The architecture typically consists of several layers, each serving specific functions** and facilitating the flow of data and control within the IoT ecosystem [5]. Here's an overview of the typical architecture of IoT:

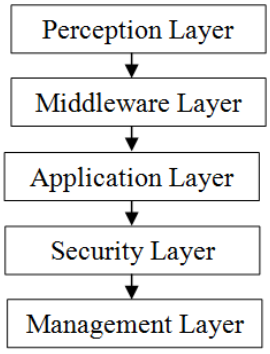

Figure 2: Architecture of IoT

Perception Layer: The perception layer, also known as the **sensing layer**, consists of IoT devices or "things" embedded with sensors, actuators and microcontrollers. Sensors collect data from the physical environment such as temperature, humidity, light, motion and pressure. Actuators enable devices to perform actions based on received data, such as **controlling switches, motors, valves, or displays**. Devices in the perception layer may include sensors, actuators, smart appliances, wearables, industrial machines, vehicles and environmental monitors.

Network Layer: The network layer facilitates **communication and connectivity between IoT devices, gateways, and other network infrastructure components**. Various connectivity technologies are used in the network layer, including Wi-Fi, Bluetooth, Zigbee, Z-Wave, cellular networks (3G/4G/5G), satellite and low-power wide-area networks **(LPWAN)**. Gateways serve as intermediaries between IoT devices and centralized systems, aggregating data from multiple devices, performing protocol translation and facilitating secure communication. Network protocols such as **MQTT, CoAP, HTTP, and AMQP** are used for data

exchange and communication between IoT devices and backend systems [6].

Middleware Layer: The middleware layer **provides services and functionalities for data processing, storage, and management** between the perception layer and the application layer. It includes components such as data brokers, message queues, event processing engines and application enablement platforms **(AEPs)**. Middleware components handle tasks such as data filtering, transformation, aggregation, routing and protocol mediation. Functions of the middleware layer may include data normalization, device management, security, authentication, authorization and access control.

Application Layer: The application layer **comprises IoT applications, services and solutions that utilize the data generated by IoT devices** to provide value-added functionalities and insights. Applications span various domains and industries, including smart homes, healthcare, transportation, agriculture, manufacturing, energy and smart cities. Examples of IoT applications include home automation systems, remote patient monitoring, asset tracking, predictive maintenance, smart grid management and traffic optimization. Application layer components may include dashboards, analytics engines, machine learning algorithms and visualization tools for data analysis, visualization and decision-making.

Security Layer: The security layer **encompasses measures and mechanisms to protect IoT devices, networks, data, and applications** from cybersecurity threats and vulnerabilities. Security measures include encryption, authentication, access control, secure bootstrapping, firmware updates and secure communication protocols. Security components may include firewalls, intrusion detection/prevention systems **(IDS/IPS)**, security gateways, device authentication servers and security management platforms. Security considerations address threats such as unauthorized access, data breaches, malware, denial-of-service **(DoS)** attacks, and privacy violations.

Management Layer: The management layer **provides capabilities for device lifecycle management, configuration, monitoring and maintenance of IoT deployments**. It includes device management platforms **(DMPs)**, network management systems **(NMS)**, and service orchestration frameworks. Management functions may include device provisioning, registration, authentication, firmware/software updates, health monitoring, troubleshooting and performance optimization. Management layer components ensure the reliability, availability, scalability, and efficiency of IoT deployments.

The architecture of IoT is characterized by its distributed nature, spanning from the edge to the cloud and involves the integration of hardware, software, networking and security components to enable seamless connectivity, data exchange and application delivery in IoT ecosystems. The architecture evolves to accom

modate new technologies, standards and use cases, driving innovation and transformation across industries and domains.

II.ROUTING IN IOT

Routing plays a crucial role in the Internet of Things (IoT) ecosystem, facilitating the transmission of data between interconnected devices within IoT networks. In IoT environments, where numerous devices are deployed to collect, process and exchange data, efficient routing mechanisms are essential to ensure reliable communication, optimize network resources and support various applications and services [7] [8]. **IoT networks consist of heterogeneous devices with diverse capabilities, operating in different environments** and communicating over a wide range of communication technologies. These devices may include sensors, actuators, controllers, and other smart objects embedded in everyday objects, machinery, infrastructure, and environments.

Routing in IoT networks involves determining the optimal paths for data packets to traverse from source devices to destination devices or services, considering factors such as network topology, device characteristics, communication constraints and application requirements. **Efficient routing protocols and algorithms are designed to address the unique challenges posed by IoT environments**, including limited bandwidth, energy constraints, dynamic network conditions, and scalability issues. The choice of routing protocol depends on various factors such as network size, density, mobility, power constraints and application-specific requirements. p**roactive, reactive and hybrid routing protocols are commonly used in IoT networks**, each offering trade-offs between overhead, latency, energy consumption and scalability.

In addition to traditional routing protocols, emerging technologies and paradigms such as edge computing, machine learning, and software-defined networking **(SDN)** are reshaping the landscape of IoT routing, enabling more adaptive, intelligent and context-aware routing solutions. These advancements aim to improve network performance, enhance security, and support advanced IoT applications across diverse domains such as smart cities, industrial automation, healthcare, agriculture and environmental monitoring. As IoT deployments continue to grow in scale and complexity, addressing the evolving requirements and challenges of routing in IoT networks becomes increasingly important. **Research and innovation in routing protocols, optimization techniques and network management approaches are critical** for unlocking the full potential of IoT and realizing its transformative impact on various industries and societal domains.

2.1. Importance of Routing in IoT Networks

Routing plays a pivotal (key) role in the functioning and efficiency of IoT networks, holding immense importance for several reasons [9] [10]:

- ***Data Transmission:*** Routing ensures the effective transmission of data between IoT devices, enabling seamless communication within the network. **It determines the optimal paths for data packets to travel from source devices to their destinations**, considering factors like network topology, device capabilities, and communication constraints.

- ***Network Scalability:*** As IoT networks continue to expand with the proliferation of connected devices, **efficient routing mechanisms are essential for scalability**. Routing protocols that can handle a large number of devices and adapt to dynamic network conditions are crucial for accommodating the growth of IoT deployments.
- ***Resource Optimization:*** Effective routing helps optimize network resources such as bandwidth, energy and memory. By directing traffic along the most efficient paths and minimizing unnecessary overhead, routing protocols **contribute to the efficient utilization of resources, extending the lifespan of battery-powered devices** and reducing operational costs.
- ***Reliability and Fault Tolerance:*** Reliable communication is paramount in IoT applications, where data integrity and timely delivery are critical. **Routing protocols ensure the robustness of the network by providing fault tolerance mechanisms**, such as route redundancy, failover and recovery strategies, to mitigate disruptions caused by device failures, network outages, or environmental factors.
- ***Energy Efficiency:*** Many IoT devices operate on limited battery power, making energy efficiency a primary concern. **Efficient routing algorithms help conserve (save) energy by minimizing communication overhead**, reducing the number of packet transmissions, and optimizing routing paths, thereby extending the battery life of IoT devices and enhancing their sustainability.
- ***Support for Various Communication Technologies:*** IoT networks utilize diverse communication technologies ranging from short-range wireless protocols like Bluetooth and Zigbee to long-range cellular networks and LPWAN technologies such as LoRaWAN and NB-IoT. **Routing protocols need to support seamless integration and interoperability** across these heterogeneous communication technologies to ensure connectivity and data exchange among IoT devices.
- ***Quality of Service (QoS):*** Many IoT applications have specific requirements for latency, throughput and reliability. Routing plays a crucial role in meeting these QoS demands by prioritizing traffic, enforcing service-level agreements and providing mechanisms for traffic engineering and congestion control to ensure consistent performance and user experience.
- ***Security and Privacy:*** Routing protocols contribute to the security and privacy of IoT networks by **implementing authentication, encryption, access control and secure routing mechanisms**. By ensuring that data is transmitted securely and only authorized devices can access network resources, routing protocols help protect sensitive information and prevent unauthorized access or tampering.

The routing is fundamental to the operation and effectiveness of IoT networks, enabling reliable communication, resource optimization, scalability, energy efficiency and support for various applications and services. As IoT deployments continue to grow and evolve, the development of advanced routing solutions tailored to the specific requirements and challenges of IoT environments becomes increasingly crucial for realizing the full potential of IoT across diverse domains.

2.2. Challenges in Routing for IoT

Routing in IoT networks presents several challenges due to the unique characteristics and requirements of these environments [11]. Some of the key challenges include:

- **Heterogeneity of Devices: IoT networks consist of diverse devices with varying capabilities**, communication protocols and power constraints. Routing protocols need to accommodate this heterogeneity and ensure compatibility and interoperability among different types of devices.
- **Scalability:** IoT deployments often involve a large number of devices distributed over wide geographic areas. Traditional routing protocols may struggle to scale efficiently to accommodate the growing number of devices and the dynamic nature of IoT networks. Scalable routing algorithms and architectures are needed to support large-scale IoT deployments.
- **Resource Constraints: Many IoT devices are resource-constrained in terms of processing power, memory and energy**. Routing protocols must be designed to minimize resource consumption and optimize energy efficiency while maintaining reliable communication and performance.
- **Dynamic Network Conditions:** IoT networks are characterized by dynamic and unpredictable network conditions, including variable link quality, network congestion, and device mobility. Routing protocols need to adapt to these changing conditions in real-time to maintain connectivity and ensure data delivery.
- **Security and Privacy:** IoT devices are often deployed in sensitive environments where security and privacy are paramount. **Routing protocols must incorporate robust security mechanisms to protect against unauthorized access**, data breaches, and cyber-attacks. Ensuring secure and authenticated communication among devices is essential to safeguard IoT networks and the data they handle.
- **Reliability and Fault Tolerance:** IoT applications often require high levels of reliability and fault tolerance to ensure continuous operation and data delivery. Routing protocols must support fault detection, recovery and **rerouting mechanisms to mitigate disruptions caused by device failures**, network outages, or environmental factors.
- **Quality of Service (QoS):** Many IoT applications have stringent requirements for latency, throughput and packet delivery reliability. Routing protocols need to prioritize traffic based on QoS parameters and provide mechanisms for traffic engineering and congestion control to meet application-specific requirements.
- **Mobility Support:** In IoT environments with mobile devices or assets, routing protocols must support seamless handover and mobility management to maintain connectivity and preserve session continuity as devices move between different network access points or coverage areas.

Addressing these challenges requires the development of innovative routing protocols, optimization techniques, and network management strategies tailored to the specific requirements and constraints of IoT deployments. Research efforts in this area aim to enhance the scalability, efficiency,

security and reliability of routing in IoT networks to unlock the full potential of IoT across various industries and applications.

2.3. Types of IoT Networks

IoT networks encompass a variety of technologies and architectures to facilitate communication between connected devices [12] [13]. These networks can be categorized based on the range of communication, power consumption, bandwidth requirements and deployment scenarios. Here are some common types of IoT networks:

Short-Range Networks: These networks are designed for communication over short distances, typically within a confined area such as a home, building or personal space. Examples of short-range IoT networks include:

- ✓ ***Bluetooth:*** A wireless technology standard for short-range communication between devices. Bluetooth Low Energy (BLE) is commonly used in IoT applications due to its low power consumption.
- ✓ ***Zigbee :*** A low-power, low-data-rate wireless communication protocol designed for low-cost, low-complexity networks with short-range coverage. Zigbee is often used in home automation and industrial control systems.
- ✓ ***Z-Wave:*** A wireless communication protocol optimized for **low-power, low-bandwidth applications in home automation**, security systems and smart energy management.

Medium-Range Networks: These networks provide communication over longer distances compared to short-range networks, covering areas such as neighborhoods, campuses, or industrial facilities. Examples of medium-range IoT networks include:

- ***Wi-Fi:*** A popular wireless networking technology that **provides high-speed data transmission over relatively long distances**. Wi-Fi is widely used in IoT applications, including smart homes, offices, and public spaces.
- ***Thread:*** A low-power, **mesh networking protocol based on IEEE 802.15.4 standard**, designed for connecting IoT devices in residential and commercial settings. Thread offers robustness, security, and support for large-scale deployments.

Long-Range Networks: These networks are designed for communication over extended distances, covering wide geographic areas such as cities, rural areas or industrial sites. Examples of long-range IoT networks include:

- ***Cellular Networks (3G/4G/5G):*** Cellular technologies provide wide-area coverage and high-speed data transmission, making them suitable for IoT applications requiring ubiquitous connectivity and high bandwidth. Cellular IoT modules are used in applications such as asset tracking, smart meters and fleet management.
- ***LoRaWAN:*** A low-power, wide-area networking **(LPWAN)** protocol designed for long-range communication with low data rates and low power consumption. LoRaWAN is suitable for IoT deployments requiring long-range connectivity, such as smart agriculture, environmental monitoring and smart cities.
- ***NB-IoT (Narrowband IoT):*** A cellular technology standardized by the 3rd Generation Partnership Project **(3GPP)** for connecting IoT devices over cellular networks. NB-IoT offers low power consumption, deep indoor coverage and support for massive IoT deployments in urban and rural areas.

Satellite Networks: Satellite networks **provide global coverage and connectivity for IoT devices in remote or inaccessible locations** where terrestrial networks are unavailable or impractical. Satellite IoT networks offer reliable communication for applications such as maritime tracking, asset monitoring, precision agriculture, and environmental monitoring.

These types of IoT networks cater to diverse use cases and deployment scenarios, offering varying trade-offs in terms of range, bandwidth, power consumption, coverage and cost. Depending on the specific requirements of IoT applications, organizations may choose the most suitable network technology or a combination of multiple technologies to meet their connectivity needs.

III.ROUTING PROTOCOLS FOR IOT

Routing protocols are essential components of IoT networks, responsible for determining the optimal paths for data transmission between interconnected devices. These protocols play a critical role in ensuring efficient and reliable communication, optimizing network resources and supporting various IoT applications and services [14] [15]. In the context of IoT, routing protocols must address the unique challenges posed by heterogeneous devices, dynamic network conditions, resource constraints and diverse application requirements. Routing protocols for IoT networks can be broadly categorized into several types, each offering different approaches to address the specific characteristics and requirements of IoT deployments. These include proactive, reactive and hybrid routing protocols, each with its own set of advantages and trade-offs.

3.1. Proactive routing protocols

Proactive routing protocols are **a type of routing protocol used in computer networks, including IoT networks**. These protocols maintain up-to-date routing information throughout the network by periodically exchanging routing updates between devices, regardless of whether there is active data transmission or not. This proactive approach ensures that devices have pre-established routes available for data transmission, minimizing latency for data delivery. Here are some common proactive routing protocols used in IoT networks:

- ✓ **Optimized Link State Routing (OLSR):** OLSR is a proactive routing protocol specifically designed for mobile ad hoc networks (MANETs), which are characterized by dynamic topology changes and device mobility. OLSR calculates and maintains multiple routes to destinations within the network, ensuring robust connectivity even in the presence of node mobility or link failures**. OLSR uses a distributed algorithm to construct a topology map of the network**, with each

device periodically broadcasting link-state advertisements (LSAs) containing information about its neighbors and their links. Based on the received LSAs, devices construct a routing table containing the shortest paths to all destinations in the network. **OLSR reduces overhead by minimizing the number of control messages** exchanged and by maintaining only the most optimal routes in the routing table. It is suitable for IoT applications where network topology changes frequently, such as smart city deployments or industrial automation [16].

- ✓ **Destination-Sequenced Distance Vector (DSDV):** DSDV is a proactive distance-vector routing protocol that maintains a routing table at each device, containing entries for all reachable destinations in the network. Unlike traditional distance-vector protocols, **DSDV uses sequence numbers to ensure loop-free routing** and to provide a mechanism for detecting and avoiding stale routing information. In DSDV, devices periodically exchange routing updates containing their routing tables with their neighbors. Each routing table entry includes the destination address, the next-hop device, the number of hops to reach the destination, and the sequence number associated with the route. Devices use these routing updates to update their routing tables and select the most optimal routes to each destination. **DSDV is well-suited for IoT applications requiring stable and deterministic routing**, such as wireless sensor networks (WSNs) deployed in environmental monitoring or precision agriculture [17]. However, it may suffer from high overhead and convergence delays in highly dynamic or large-scale networks.

Proactive routing protocols offer benefits such as reduced latency, increased network stability, and improved fault tolerance compared to reactive routing protocols. However, they may incur higher overhead due to the periodic exchange of routing updates and may not be suitable for highly dynamic or resource-constrained IoT networks. Organizations should carefully consider the requirements of their IoT applications and the characteristics of their network environments when selecting a routing protocol.

3.2. Reactive Routing Protocols

Reactive routing protocols are **another type of routing protocol commonly used in computer networks, including IoT networks**. Unlike proactive routing protocols that maintain up-to-date routing information regardless of network activity, reactive routing protocols establish routes on-demand, only when data needs to be transmitted between source and destination devices. **This on-demand approach helps conserve network resources by minimizing the overhead** associated with maintaining routing information for inactive routes [18]. Here are some common reactive routing protocols used in IoT networks:

- ✓ **Ad-hoc On-demand Distance Vector (AODV):** AODV is a reactive routing protocol designed for mobile ad hoc networks (MANETs) and IoT environments characterized by dynamic topology changes and device mobility. **AODV establishes routes between devices only when data needs to be transmitted**, rather than maintaining pre-established routes as in proactive routing protocols. When a device needs to send data to a destination for which it does not have a route, it initiates a route discovery process by broadcasting a route request (RREQ) packet to its neighbors. Each intermediate device receiving the RREQ forwards it to its neighbors until the RREQ reaches the destination or an intermediate device with a route to the destination. Upon receiving the RREQ, devices along the route **create reverse path entries in their routing tables to facilitate route establishment**. Once the destination or an intermediate device with a route to the destination is reached, a route reply (RREP) packet is sent back to the source along the reverse path. The source device then caches the route and can begin transmitting data using the established route. AODV offers benefits such as low routing overhead, **rapid route discovery and support for both unicast and multicast communication**. It is suitable for IoT applications where devices are frequently moving or joining/leaving the network, such as mobile sensor networks or disaster response scenarios.
- ✓ **Dynamic Source Routing (DSR):** DSR is another reactive routing protocol **commonly used in mobile ad hoc networks (MANETs) and IoT deployments**. DSR allows devices to maintain route caches containing routes learned from previous communications. When a device needs to transmit data to a destination, it consults its route cache to find a suitable route. **If a route is not available in the cache, the device initiates a route discovery process similar to AODV**. Route discovery in DSR involves broadcasting a route request (RREQ) packet to find a route to the destination. Devices that receive the RREQ forward it to their neighbors until the RREQ reaches the destination or an intermediate device with a route to the destination. Once the route is discovered, a route reply (RREP) packet is sent back to the source along the discovered route. DSR offers benefits such as route optimization, reduced routing overhead and support for multiple route options. However, it may suffer from high overhead in large-scale networks or networks with frequent topology changes.

Reactive routing protocols offer benefits such as reduced routing overhead, scalability and adaptability to dynamic network conditions compared to proactive routing protocols. However, they may incur delays in route discovery and setup, particularly in networks with high mobility or frequent topology changes. Organizations should carefully evaluate the requirements of their IoT applications and the characteristics of their network environments when selecting a routing protocol.

3.3. Hybrid Routing Protocols

Hybrid routing protocols combine elements of both proactive and reactive routing approaches to achieve a balance between route availability and resource efficiency. These protocols leverage proactive techniques for maintaining frequently used routes while employing reactive techniques for dynamic or infrequently used routes. **Hybrid routing protocols aim to address the specific challenges and requirements of IoT networks** by offering flexibility, scalability and adaptability to varying network conditions [19] [20]. Here are some common hybrids routing protocols used in IoT networks:

- ✓ **Zone Routing Protocol (ZRP): ZRP divides the network into zones, with each device responsible for maintaining routing information** within its zone. Within each zone, proactive routing techniques are used to establish and maintain routes between devices. Devices periodically exchange routing updates containing information about routes within their zones to ensure route availability and stability. When a device needs to communicate with a device outside its zone, it initiates a route discovery process similar to reactive routing protocols. **A route request (RREQ) packet is broadcasted to neighboring zones**, and devices along the border of the source zone forward the RREQ to neighboring zones until a route to the destination is found. Once the route is established, data can be transmitted using the discovered route. **ZRP offers benefits such as reduced routing overhead within zones, rapid route discovery** across zones, and scalability to large networks. It is suitable for IoT deployments where devices are organized into logical groups or clusters, such as smart grid networks or distributed sensor networks.
- ✓ **Hierarchical Routing Protocol (HRP): HRP organizes devices into a hierarchical structure with multiple levels of routing hierarchy**, similar to the layered architecture of the Internet. Each level of the hierarchy corresponds to a different scope or domain within the network, such as local area networks (LANs), regional networks or global networks. Proactive routing techniques are used within each level of the hierarchy to maintain routing information and establish routes between devices within the same level. When a device needs to communicate with a device in a different level of the hierarchy, a route discovery process similar to reactive routing protocols is initiated. **HRP offers benefits such as reduced routing overhead within each level of the hierarchy**, hierarchical addressing and routing, and scalability to large and geographically distributed networks. It is suitable for IoT deployments with hierarchical or federated architectures, such as smart city networks or industrial automation systems. Hybrid routing protocols offer advantages such as reduced routing overhead, rapid route discovery, scalability and adaptability to dynamic network conditions. By combining proactive and reactive routing techniques, **these protocols provide flexibility and efficiency in managing routes in IoT networks**. Organizations should carefully consider the requirements of their IoT applications and the characteristics of their network environments when selecting a routing protocol.

In summary, routing protocols play a crucial role in enabling efficient and reliable communication in IoT networks. By selecting and deploying appropriate routing protocols based on the specific requirements and constraints of IoT applications, organizations can ensure optimal performance, scalability, and resource utilization in their IoT deployments.

3.4. Routing protocols in the Internet of Things (IoT)

Routing protocols in the Internet of Things (IoT) play a crucial role in facilitating communication between interconnected devices and ensuring efficient data transmission within IoT networks. **These protocols determine the optimal paths for data to travel from source to destination**, considering factors such as network topology, device capabilities, energy efficiency, and quality of service requirements [21]. Here are some common routing protocols used in IoT:

a) RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks): RPL is a widely adopted routing protocol **designed specifically for low-power and lossy networks (LLNs)**, which are characteristic of many IoT deployments. It operates on top of the IPv6 protocol suite and is optimized for resource-constrained devices with limited processing power, memory and energy. Low-power and Lossy Networks (LLNs) are a type of network typically found in environments where devices have limited power sources, processing capabilities, and communication bandwidth [22]. These networks are commonly associated with the Internet of Things (IoT) deployments and sensor networks.

- ***Limited Power Resources:*** Devices in LLNs are often battery-powered or have limited access to power sources. As a result, energy efficiency is a critical consideration in the design of LLN protocols and algorithms. Devices may utilize low-power communication technologies such as IEEE 802.15.4, Bluetooth Low Energy (BLE) or LoRaWAN to conserve energy.
- ***Lossy Communication Links:*** LLNs are characterized by communication links that are prone to packet loss, high latency and low throughput. This could be due to factors such as interference, signal attenuation or the use of low-power communication technologies. Protocols designed for LLNs must be resilient to such challenges and able to maintain connectivity despite intermittent communication.
- ***Topology Formation:*** LLNs often employ techniques for self-organization and dynamic topology formation. Devices may form ad-hoc networks or organize themselves into hierarchical structures to optimize communication and routing efficiency. Protocols like RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) establish Directed Acyclic Graphs (DAGs) to represent network topologies. Topology formation in low-power and lossy networks (LLNs) involves the creation and maintenance of a network structure that facilitates efficient communication among devices despite their limitations in power, processing capabilities and communication bandwidth. LLNs often operate in dynamic environments where devices may join or leave the network unpredictably. In such cases, devices need to autonomously form ad-hoc networks without relying on pre-existing infrastructure or centralized coordination. Ad-hoc formation allows devices to establish direct or multi-hop communication links with nearby neighbors. In large-scale LLNs, hierarchical organization may be employed to improve scalability and efficiency. Devices may organize themselves into clusters or domains, with each cluster having a designated cluster head or border router responsible for intra-cluster communication and inter-cluster routing.

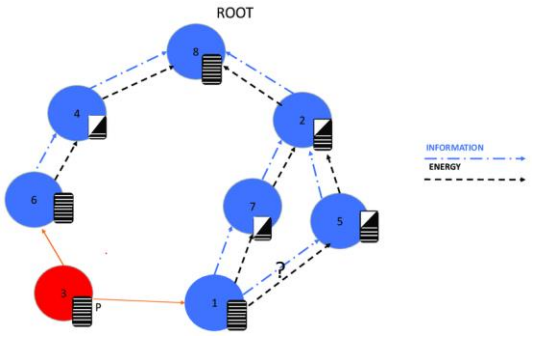

Figure 3: LLN Network Model

Hierarchical organization helps reduce overhead and control traffic in large networks. Devices in LLNs perform neighbor discovery to identify and establish communication links with neighboring devices. Neighbor discovery mechanisms may involve periodic beaconing, listening for broadcast announcements, or exchanging hello messages. Once neighboring devices are discovered, devices may exchange information about network parameters such as link quality and available resources. Assessing the quality of communication links is crucial in LLNs, where links are often prone to packet loss, latency and interference shown in Figure 3. Devices may use techniques such as link probing, packet reception ratio estimation or signal strength measurement to evaluate link quality. This information helps in selecting reliable paths for routing and avoiding unreliable links.

Topology control mechanisms may be employed to optimize network connectivity and reduce energy consumption. For example, devices may adjust transmission power, channel selection or duty cycles to maintain connectivity while minimizing interference and energy expenditure. Topology control helps in mitigating network congestion, reducing collisions, and extending network lifetime. LLNs often utilize dynamic routing protocols such as RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) to adapt to changing network conditions and device mobility. Dynamic routing protocols establish and maintain routing paths based on real-time information about network topology, link quality, and device status. This allows for efficient and robust communication even in highly dynamic environments. Routing in LLNs is typically managed by specialized protocols like RPL, which are optimized for low-power and lossy environments. These protocols use objective functions to select routes based on metrics such as energy consumption, latency, and link quality. Routing decisions are often made locally by individual devices to adapt to changing network conditions. RPL uses a destination-oriented directed acyclic graph (DODAG) structure to organize network topology and determine routing paths. It supports both proactive and reactive routing strategies, allowing devices to maintain pre-established routes while also enabling on-demand route discovery. RPL is suitable for various IoT applications, including smart homes, industrial automation, building automation and environmental monitoring.

b). 6LoWPAN Routing Protocol (6LoWPAN-RP): 6LoWPAN-RP is a routing protocol **designed for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)**, which are commonly used in IoT deployments. It enables IPv6 packets to be transmitted over low-power wireless networks with constrained bandwidth and energy resources. 6LoWPAN-RP supports both proactive and reactive routing mechanisms, providing flexibility in adapting to dynamic network conditions [23]. **The protocol is lightweight and scalable, making it suitable for large-scale IoT deployments** with thousands or even millions of interconnected devices. 6LoWPAN-RP is often used in smart energy systems, smart cities, healthcare monitoring and agricultural monitoring applications.

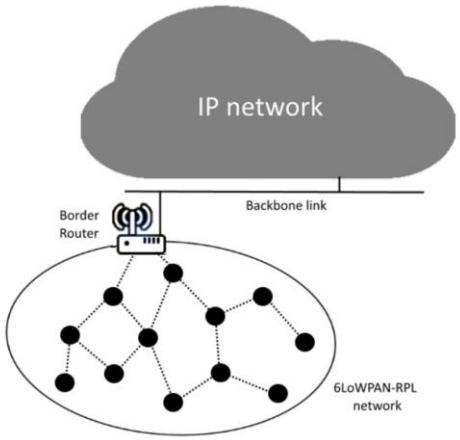

Figure 4: 6LoWPAN Network Architecture

Figure 4, the 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) network architecture is tailored to **facilitate IPv6 packet transmission over low-power wireless networks**, specifically designed for IoT and sensor network applications. Operating over various low-power wireless technologies like IEEE 802.15.4, Bluetooth Low Energy (BLE) and LoRaWAN, 6LoWPAN defines an adaptation layer that sits between the link and network layers. This adaptation layer handles packet fragmentation, header compression and address auto-configuration to adapt IPv6 packets to the constraints of low-power networks. Fragmentation divides IPv6 packets into smaller units to fit within the maximum transmission unit **(MTU)** of the underlying link layer, while header compression techniques, such as Context-Based Compression, minimize IPv6 header overhead to conserve bandwidth. Additionally, 6LoWPAN devices may employ techniques like Stateless Address Auto configuration for dynamic IPv6 address assignment. At the network layer, **IPv6 provides end-to-end connectivity, enabling devices to have unique global addresses and communicate over the Internet**. While 6LoWPAN itself doesn't specify a routing protocol, it can work alongside protocols like RPL for routing in large-scale low-power wireless networks. At the application layer, various protocols for sensor data collection, home automation and other IoT applications can run over 6LoWPAN-enabled devices, extending the reach of IPv6-based networks to diverse IoT deployments and enhancing interoperability, scalability and energy efficiency.

c) AMQP (Advanced Message Queuing Protocol): AMQP is a messaging protocol commonly used in IoT deployments to **facilitate communication between devices and backend systems**. While not a traditional routing protocol, AMQP provides features for message queuing, routing, and delivery assurance, making it suitable for IoT environments. AMQP

enables devices to publish messages to queues and subscribe to messages from queues, allowing for asynchronous communication and decoupling of sender and receiver. **It supports advanced routing features such as topic-based routing**, where messages are routed based on specified criteria or message attributes [24]. AMQP is used in various IoT applications, including remote monitoring, asset tracking, logistics management and industrial automation.

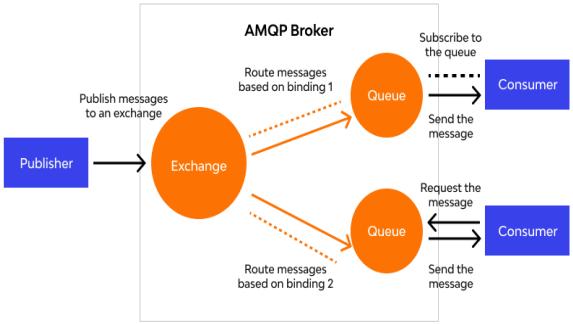

Figure 5: AMQP (Advanced Message Queuing Protocol) Architecture

In figure 5, the Advanced Message Queuing Protocol (AMQP) architecture is designed to facilitate robust and efficient messaging between distributed applications or systems. At its core are producers, which generate messages to be sent to AMQP brokers. These brokers serve as intermediaries responsible for mediating message routing and delivery. Messages from producers are directed to exchanges, which receive them and route them to one or more queues based on predefined routing rules. Queues store messages temporarily until they are consumed by consumer applications, which retrieve messages from queues for processing. Bindings establish the relationship between exchanges and queues, defining how messages are routed within the AMQP infrastructure. Consumers subscribe to queues and receive messages in a pull-based manner, processing them according to application logic. **AMQP brokers support various message delivery patterns** and provide features such as message acknowledgment, ensuring reliable message transmission. Channels enable multiplexed communication streams between AMQP clients and brokers within a connection, reducing overhead and optimizing resource utilization. Additionally, virtual hosts provide logical isolation and partitioning within brokers, allowing multiple independent messaging environments to coexist within a single physical instance. Overall, the **AMQP architecture offers a flexible and scalable framework** for building distributed messaging systems, enabling seamless communication between applications or services in diverse deployment scenarios.

d) MQTT (Message Queuing Telemetry Transport):

MQTT is a lightweight messaging protocol commonly used in IoT deployments for efficient, low-latency communication between devices and applications. While not a routing protocol in the traditional sense, **MQTT supports for publish-subscribe messaging pattern, where devices publish messages to topics** and subscribers receive messages from topics they are interested in. **MQTT brokers act as intermediaries that route messages between publishers and subscribers**, enabling scalable and reliable communication in IoT networks. MQTT's lightweight nature and support for Quality of Service (QoS) levels make it suitable for IoT applications with constrained devices and intermittent connectivity [25]. MQTT is widely used in smart home automation, remote monitoring, telemetry, and machine-to-machine (M2M) communication applications.

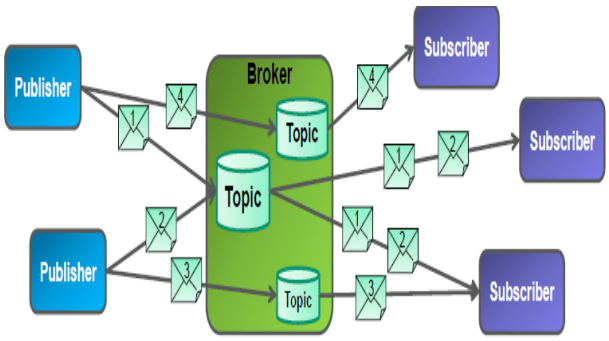

Figure 6: MQTT (Message Queuing Telemetry Transport) Architecture

In figure 6, the MQTT (Message Queuing Telemetry Transport) architecture revolves around a lightweight messaging protocol designed to facilitate efficient communication among devices, particularly in scenarios with limited bandwidth, high latency, or unreliable networks. At its core, MQTT employs a client-server model, where clients connect to a central intermediary known as the broker to exchange messages. Clients, which can range from IoT devices to mobile applications, act as either publishers, sending messages, or subscribers, receiving messages. Communication occurs through the publication and subscription to topics, which serve as hierarchical strings categorizing messages. The broker, responsible for message routing and client management, facilitates this exchange, handling client connections and managing subscriptions. Messages, containing payloads and optional metadata, are transmitted between clients via the broker. **MQTT supports multiple Quality of Service (QoS) levels, allowing for varying degrees of message delivery assurance**. Additionally, features like retained messages and Last Will and Testament (LWT) ensure reliability and enable efficient handling of client status changes. Overall, MQTT's straightforward yet versatile architecture makes it a preferred choice for IoT deployments and messaging applications where resource efficiency and reliable communication are paramount.

e) CoAP (Constrained Application Protocol):

CoAP is a lightweight application-layer protocol designed for constrained devices and low-bandwidth, high-latency networks. **It is used for communication between IoT devices and is commonly used in conjunction with UDP** or SMS transport protocols [26]. CoAP supports RESTful principles, making it suitable for accessing and manipulating resources on **IoT devices using HTTP-like methods such as GET, PUT, POST and DELETE**. While not a routing protocol per se, CoAP can be used to exchange control

messages between devices and to interact with routing protocols for configuration, monitoring, and management.

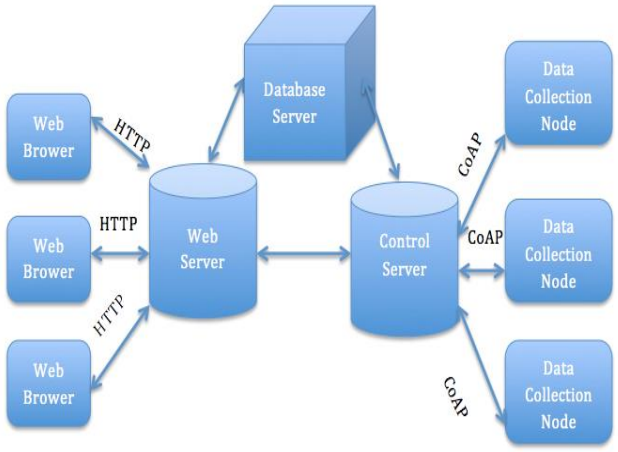

Figure 7: CoAP (Constrained Application Protocol) Architecture

In figure 7, architecture of the Constrained Application Protocol (CoAP) is structured to address the unique challenges of communication in the Internet of Things (IoT) ecosystem, where devices often possess limited processing power, memory, and energy resources. CoAP adheres to a client-server model, mirroring the familiar paradigm of HTTP, where clients initiate requests and servers respond accordingly. However, CoAP is distinct in its use of the lightweight User Datagram Protocol (UDP), optimizing communication for constrained networks by minimizing overhead. CoAP employs RESTful principles, enabling interactions with resources through standard HTTP-like methods such as GET, POST, PUT, and DELETE. A notable feature is its support for observing resources, facilitating efficient event-driven communication by allowing clients to subscribe to changes in resource state. **CoAP also offers optional reliability mechanisms at the message layer, ensuring robust message delivery** over unreliable networks, while including congestion control to manage network traffic. Furthermore, **CoAP utilizes a compact binary message format to minimize data size and processing demands**, which is crucial for efficient operation on resource-constrained devices. This architecture collectively positions CoAP as a suitable protocol for IoT applications, offering lightweight communication, resource efficiency, and support for RESTful interactions tailored to constrained networks and devices.

f) BLE (Bluetooth Low Energy) Mesh:

BLE mesh is a routing protocol used in Bluetooth Low Energy networks to enable communication between devices in a mesh topology. It allows devices to relay messages to reach destinations that are out of direct range, extending the coverage area of BLE networks. **BLE mesh is commonly used in applications such as smart home automation, asset tracking** and indoor positioning systems. These are just a few examples of routing protocols commonly used in IoT deployments [27]. The choice of routing protocol depends on various factors such as network topology, device capabilities, application requirements, scalability, and energy efficiency considerations. Organizations deploying IoT solutions must carefully evaluate their requirements and select the most appropriate routing protocol to ensure reliable and efficient communication within their IoT networks.

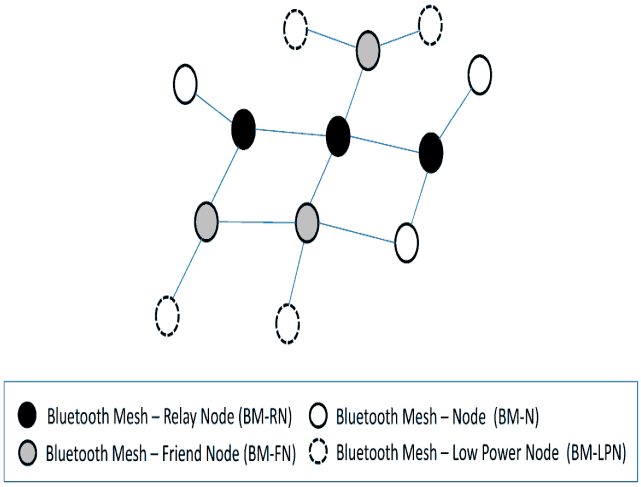

Figure 8: BLE (Bluetooth Low Energy) Mesh Architecture

Figure 8, architecture of Bluetooth Low Energy (BLE) Mesh networks revolves around a decentralized mesh topology, offering a robust and energy-efficient solution for connecting a multitude of low-power IoT devices. In this architecture, devices within the network, termed nodes, assume multiple roles such as low-power nodes, relay nodes, proxy nodes, friend nodes, and gateways. Low-power nodes typically serve as sensors or actuators, intermittently waking up to perform tasks while conserving energy in sleep mode. **Relay nodes act as intermediaries, extending the communication range by relaying messages between nodes**. Proxy nodes bridge the BLE Mesh network with external networks, enabling connectivity to the internet or local networks. Friend nodes store messages for low-power nodes, allowing them to conserve energy by remaining in a low-power state until needed. Gateways facilitate communication between the BLE Mesh network and external systems, enabling data exchange with cloud services or other IoT platforms. Communication in BLE Mesh networks follows a publish-subscribe model, where nodes publish messages to specific topics or groups, and interested nodes subscribe to receive relevant messages. Overall, **the BLE Mesh architecture prioritizes scalability, reliability, and energy efficiency, making it well-suited for diverse IoT** applications requiring large-scale deployment of low-power devices.

IV. QOS ROUTING IN IOT

Quality of Service (QoS) routing is a network routing strategy that **prioritizes certain types of traffic or data streams based on predefined QoS metrics and parameters**. Unlike traditional routing, which focuses solely on finding the shortest or most efficient path for data transmission, QoS routing takes into account additional factors such as latency, packet loss, throughput, jitter and reliability. In QoS routing, routes are selected based on their ability to meet specified QoS requirements, ensuring that critical data packets receive preferential treatment over less important or non-real-time traffic. **QoS routing algorithms aim to optimize network performance by dynamically adjusting routing decisions** to accommodate changing network conditions and QoS constraints. The goal of QoS routing is to guarantee a certain

level of performance and service quality for applications and services that require timely, reliable and efficient data delivery [28] [29]. By prioritizing traffic based on QoS parameters, QoS routing helps maximize the utilization of network resources, minimize congestion, reduce latency and improve overall user experience in communication networks, including Internet of Things (IoT) environments.

4.1. The importance of Quality of Service (QoS)

The importance of Quality of Service (QoS) in Internet of Things (IoT) networks cannot be overstated, as it directly impacts the reliability, efficiency, and performance of IoT applications and services [30]. Several key reasons highlight the significance of QoS in IoT environments:

- ***Reliability:*** Many IoT applications, such as remote monitoring in healthcare, industrial automation and smart grids, rely on real-time data transmission and require high levels of reliability. QoS mechanisms ensure that critical data packets are delivered promptly and reliably, minimizing the risk of data loss or transmission errors.
- ***Timeliness:*** In IoT deployments, timely data delivery is essential for supporting time-sensitive applications and services. QoS mechanisms prioritize real-time or high-priority traffic, reducing latency and ensuring that data reaches its destination within specified time constraints. This is particularly crucial for applications such as autonomous vehicles, where delays in data transmission can have safety implications.
- ***Resource Efficiency:*** QoS mechanisms optimize the utilization of network resources, such as bandwidth, processing power, and energy, by dynamically allocating resources based on application requirements. By efficiently managing resources, QoS ensures that IoT networks operate at peak performance while minimizing waste and congestion.
- ***User Experience:*** QoS directly influences the end-user experience in IoT applications by ensuring consistent and predictable performance. By delivering high-quality service with minimal latency and packet loss, QoS enhances user satisfaction and enables seamless interaction with IoT devices and services.
- ***Scalability:*** As IoT deployments continue to grow in scale and complexity, QoS becomes increasingly important for maintaining network scalability and performance. QoS mechanisms enable IoT networks to scale efficiently by dynamically adapting to changing network conditions, accommodating new devices and optimizing resource allocation.
- ***Compliance and Regulation:*** In certain industries, such as healthcare, finance and transportation, regulatory requirements mandate specific QoS standards to ensure data privacy, security and reliability. Compliance with these regulations is essential for IoT deployments to operate legally and securely.

QoS plays a critical role in ensuring the success and effectiveness of IoT deployments by guaranteeing reliable, efficient and timely data transmission. By prioritizing QoS considerations in the design and management of IoT networks, organizations can maximize the value and impact of their IoT initiatives across various industries and applications.

4.2. Challenges and Considerations of QoS Routing in IoT

Quality of Service (QoS) routing in Internet of Things (IoT) networks faces several challenges and considerations due to the unique characteristics and requirements of IoT environments. **Addressing these challenges is essential for ensuring reliable, efficient and high-performance communication in IoT deployments** [31]. Some of the key challenges and considerations of QoS routing in IoT include:

- ***Heterogeneity of Devices:*** IoT networks consist of diverse devices with varying capabilities, communication technologies and QoS requirements. **QoS routing algorithms must account for this heterogeneity a**nd adapt routing decisions to accommodate different types of devices and traffic patterns.
- ***Scalability:*** As IoT deployments continue to grow in scale and complexity, QoS routing protocols must scale efficiently to support large numbers of devices and data flows. **Scalability challenges arise from the need to maintain QoS requirements** while minimizing overhead and resource consumption.
- ***Resource Constraints:*** Many IoT devices are resource-constrained in terms of processing power, memory, and energy. **QoS routing algorithms must optimize resource usage to minimize energy consumption** and extend the battery life of devices, while still ensuring QoS objectives are met.
- ***Dynamic Network Topologies:*** IoT networks are characterized by dynamic and unpredictable network topologies due to factors such as device mobility, intermittent connectivity, and environmental changes. **QoS routing protocols must be capable of adapting to these dynamic conditions** and dynamically adjusting routing decisions in real-time.
- ***QoS Metrics and Trade-offs:*** QoS routing involves optimizing multiple QoS metrics such as latency, packet loss, throughput, and jitter. However, these metrics are often interrelated and optimizing one metric may come at the expense of others. QoS routing algorithms must balance trade-offs between different QoS metrics to achieve overall performance objectives.
- ***QoS Provisioning and Management:*** Effective **QoS provisioning and management require mechanisms for measuring, monitoring and enforcing QoS requirements** in IoT networks. This includes mechanisms for traffic classification, admission control, congestion management and traffic shaping to ensure that QoS objectives are met under varying network conditions.
- ***Security and Privacy:*** QoS routing protocols must address security and privacy concerns to protect sensitive IoT data from unauthorized access, interception and tampering. Secure and authenticated communication mechanisms are **essential for ensuring the integrity and confidentiality of data transmitted over IoT networks**.
- ***Standardization and Interoperability:*** The lack of standardized QoS routing protocols and interoperability between different IoT devices and platforms poses

challenges for seamless communication and integration in heterogeneous IoT environments. **Standardization efforts are needed to promote interoperability** and compatibility among IoT devices and systems.

V.FUTURE TRENDS AND CHALLENGES IN ROUTING FOR IOT

Routing for IoT	Trend	Challenge
Edge Computing and Edge Routing	With the increasing deployment of edge computing infrastructure in IoT networks, there's a growing trend towards performing data processing and routing at the network edge. Edge routing involves distributing routing functions to edge devices or edge computing nodes, enabling faster response times, reduced latency and improved bandwidth utilization.	Edge routing introduces new challenges such as resource constraints, dynamic network conditions and heterogeneity of edge devices. Designing efficient and scalable edge routing algorithms that can adapt to diverse edge environments and optimize routing decisions based on local context and constraints is crucial.
Machine Learning for Routing Optimization	Machine learning (ML) techniques are being applied to optimize routing decisions in IoT networks. ML algorithms can analyze historical data, network traffic patterns, and environmental conditions to predict optimal routing paths, mitigate congestion and improve overall network performance.	Leveraging ML for routing optimization requires robust data collection, feature engineering and model training processes. Additionally, ensuring the reliability, interpretability, and scalability of ML-based routing solutions remains a challenge. Addressing these challenges will be crucial for realizing the full potential of ML in routing optimization for IoT networks.
Integration with 5G Networks	The rollout of 5G networks promises to revolutionize IoT connectivity by offering higher data rates, lower latency, and greater reliability. Integrating IoT routing protocols with 5G networks enables seamless connectivity, enhanced mobility support and support for massive IoT deployments.	Integrating IoT routing protocols with 5G networks requires addressing interoperability issues, standardizing communication protocols and ensuring seamless handover between different radio access technologies. Additionally, optimizing routing protocols for the unique characteristics of 5G networks, such as network slicing and multi-access edge computing **(MEC)**, presents new challenges.

VI.CONCLUSION

In conclusion, this investigation on routing for Internet of Things (IoT) has provided valuable insights into the fundamental concepts, protocols and strategies employed in routing data within IoT networks. Throughout the study, we have explored the importance of routing in facilitating communication among IoT devices, ensuring efficient data transmission, and optimizing network performance. Firstly, we discussed the fundamentals of routing in IoT, including the definition of routing, its role in data transmission, and the unique requirements and challenges associated with routing in IoT environments. We examined various routing protocols, including proactive, reactive and hybrid protocols, highlighting their characteristics, advantages, and limitations. Furthermore, this analysis delved into energy-efficient routing strategies tailored for IoT deployments, recognizing the energy constraints inherent in IoT devices and the importance of optimizing energy usage to prolong device lifetime and improve overall network efficiency. Techniques such as sleep scheduling, energy-aware path selection and load balancing have discussed in detail, along with case studies illustrating their effectiveness in conserving energy. Moreover, the study addressed Quality of Service (QoS) routing in IoT, emphasizing the significance of delivering data with specific QoS requirements such as latency, reliability and throughput. QoS-aware routing protocols and mechanisms have been examined, highlighting their role in meeting diverse QoS objectives and ensuring satisfactory user experiences in IoT applications.

VII.REFERENCES

[1]. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer networks, 54(15), 2787-2805.

[2]. Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. ACM SIGCOMM computer communication review, 24(4), 234-244.

[3]. Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol (OLSR). IETF RFC 3626.

[4]. Chakrabarti, S., & Mishra, S. (2014). Routing protocols in wireless sensor networks: a survey. In Wireless Networks and Security (pp. 53-77). Springer, New Delhi.

[5]. Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. Mobile Computing, 153(5), 353-373.

[6]. Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) routing. IETF RFC 3561.

[7]. Kahn, J. M., Katz, R. H., & Pister, K. S. (1999). Next century challenges: Mobile networking for smart dust. In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (pp. 271-278).

[8]. Raza, S., & Zeadally, S. (2019). Internet of Things (IoT) routing protocols: Review, taxonomy, and future directions. Journal of Network and Computer Applications, 126, 65-84.

[9]. Sommer, C., & Dressler, F. (2011). The need for cooperation and communication in vehicular networks. IEEE Wireless Communications, 17(6), 37-44.

[10]. Kim, S., & Park, J. (2018). Performance analysis of CoAP, MQTT, and MQTT-SN in IoT-based applications. International Journal of Distributed Sensor Networks, 14(9), 1550147718801223.

[11]. Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100).

[12]. Hu, W., Chen, Y., Wang, F., & Xie, C. (2018). Energy-efficient routing for wireless sensor networks based on a genetic algorithm. Computers, Materials & Continua, 57(1), 83-96.

[13]. Jia, X., & Ma, J. (2015). A survey on energy-efficient routing protocols in wireless sensor networks. Journal of Computer and Communications, 3(11), 182-189.

[14]. Zamora, M. A., & Rassau, A. (2012). An energy-aware routing protocol for ad hoc networks with node constraints. Computer Networks, 56(1), 278-289.

[15]. Guo, Z., Liu, Y., Hu, J., & Zhou, X. (2019). An energy-efficient routing protocol for wireless sensor networks using fuzzy-logic-based decision making. Wireless Networks, 25(4), 1763-1775.

[16]. Xie, K., Niu, Y., & Xie, S. (2014). Energy-efficient routing algorithm based on ant colony optimization for wireless sensor networks. Sensors, 14(5), 8755-8774.

[17]. Chen, H., & Ku, T. H. (2011). Routing in IoT: QoS-Oriented research trends and directions. In 2011 IEEE International Conference on Service-Oriented Computing and Applications (pp. 195-202).

[18]. Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2013). Adaptive application-layer protocol for reliable communication in IoT. In 2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (pp. 142-147).

[19]. Tilak, S., Abu-Ghazaleh, N. B., & Heinzelman, W. B. (2002). A taxonomy of wireless micro-sensor network models. ACM SIGMOBILE Mobile Computing and Communications Review, 6(2), 28-36.

[20]. Jara, A. J., Genoud, D., & Bocchi, Y. (2016). Analysis of routing protocols for Internet of Things. In Proceedings of the 1st ACM Workshop on Middleware for Context-Aware Applications in the IoT (pp. 3-8).

[21]. Hossain, E., & Hasan, M. (2018). Routing protocols in Internet of Things: A survey. In 2018 IEEE Region 10 Symposium (TENSYMP) (pp. 508-513).

[22]. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., & Vasseur, JP. (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. Retrieved from https://tools.ietf.org/html/rfc6550

[23]. Shelby, Z., & Chakrabarti, S. (2011). 6LoWPAN: The Wireless Embedded Internet. Wiley.

[24]. Apache Software Foundation. (n.d.). Apache Qpid. Retrieved from http://qpid.apache.org

[25]. OASIS Standard. (2014). MQTT Version 3.1.1. Retrieved from https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/

[26]. Shelby, Z., Hartke, K., & Bormann, C. (2014). The Constrained Application Protocol (CoAP). RFC 7252. Retrieved from https://tools.ietf.org/html/rfc7252

[27]. Bluetooth Special Interest Group (SIG). (n.d.). Bluetooth Mesh. Retrieved from https://www.bluetooth.com/specifications/mesh-specifications/

[28]. Garcia-Sanchez, A. J., Garcia-Sanchez, F., Losilla, F., Garcia-Haro, J., & Rodriguez, R. (2012). A comprehensive review on intelligent wireless sensor networks. Wireless Communications and Mobile Computing, 12(14), 1231-1258.

[29]. Sahoo, A. R., & Rajput, A. (2019). A comprehensive study of routing protocols for the Internet of Things. In Proceedings of the 3rd International Conference on Intelligent Computing and Control Systems (ICICCS 2019) (pp. 637-643).

[30]. Xu, H., Zhang, W., & Liu, A. (2019). A survey on routing protocols in the Internet of Things. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 614-618).

[31]. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

ABOUT THE AUTHORS

Dr.D.Maruthanayagam received his **Ph.D** Degree from Manonmaniam Sundaranar University, Tirunelveli in the year 2014. He received his **M.Phil** Degree from Bharathidasan University, Trichy in the year 2005. He received his **M.C.A** Degree from Madras University, Chennai in the year 2000. He is working as **Dean cum Professor**, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above **22 years** of experience in academic field. He has published **7 books**, more than **60 papers** in International Journals and **35 papers** in National & International Conferences so far. His areas of interest include Computer Networks, Grid Computing, Cloud Computing and Mobile Computing.

S.Bharathi received her **M.phil** Degree from Sri Vijay Vidyalaya College of Arts and Science, Nallampalli, Dharmapuri in the Year 2018. She has received her **M.Sc.,** Degree from Sri Vijay Vidyalaya College of Arts and Science, Nallampalli, Dharmapuri in the year 2016. She is pursuing her **Ph.D** Degree (Full Time) in Sri Vijay Vidyalaya College of Arts and Science, Nallampalli, Dharmapuri, Tamilnadu, India. Her Current research of interests includes Internet of Things, Cloud Computing, Network Security and Cryptography.