Paper Type: Original Article

Energy-Efficient Protocols for IoT Devices

Neelu Kumari, Parul Kumari, Saket Kumar
School of Computer Science Engineering, KIIT University, Bhubaneswar, India ; 22052647@kiit.ac.in ; 22052652@kiit.ac.in ; 22054212@kiit.ac.in

Citation:

Received: 22 August 2024 *Revised: 2 October 2024* *Accepted: 11* Nov *2024*	Neelu Kumari, Parul Kumari, Saket Kumar (2024).Energy-Efficient Protocols for IoT Devices. 1-18

Abstract

The Internet of Things (IoT) is revolutionizing our world by connecting everyday objects to the internet, but this increased connectivity comes with a growing energy demand. Research papers in your Google Drive address this challenge by exploring energy-efficient solutions for IoT networks, particularly Wireless Sensor Networks (WSNs). These papers investigate various approaches to optimize energy consumption in WSNs, including clustering algorithms, energy-aware routing protocols, energy harvesting techniques, and sleep mode technologies. These research efforts aim to create a more sustainable IoT ecosystem by addressing the crucial challenge of energy efficiency.

Keywords: Internet of Things (IoT), Wireless Sensor Networks (WSNs), energy efficiency, energy consumption, sustainability, green IoT, network lifetime, data transmission, routing protocols, clustering algorithms, sleep mode, duty cycling, energy harvesting

1 | Introduction

The Internet of Things (IoT) is rapidly transforming the world around us, permeating every facet of our lives and revolutionizing the way we interact with technology and the physical world. By connecting a vast array of devices to the internet, from everyday objects like household appliances and wearable sensors to complex industrial machines and critical infrastructure components, the IoT is creating an interconnected network of intelligent systems capable of collecting, exchanging, and processing data on an unprecedented scale. This paradigm shift has the potential to revolutionize various sectors, including healthcare, transportation, manufacturing, agriculture, and environmental monitoring, by enabling smarter, more efficient, and data-driven decision-making.[1, 2, 3, 5, 4]

At the heart of this transformative technology lie Wireless Sensor Networks (WSNs), which serve as the fundamental building blocks of many IoT applications. WSNs typically comprise numerous small, resource-constrained sensor nodes deployed in diverse environments to monitor physical phenomena and transmit data wirelessly. These nodes act as the eyes and ears of the IoT, gathering crucial information about the world around us, from temperature and humidity levels to pressure, motion, and location data. The data collected by WSNs is then transmitted to central processing units or cloud platforms for analysis and decision-making, enabling a wide range of applications, including environmental monitoring, smart agriculture, industrial automation, and smart cities.[1, 2, 3, 5, 4]

However, the widespread deployment of WSNs and the exponential growth of connected devices in the IoT ecosystem bring forth a critical challenge: energy consumption. As billions of devices join the network, often powered by batteries

Corresponding Author:22052652@kiit.ac.in

with limited lifespans, ensuring energy efficiency becomes paramount. This is particularly crucial for WSNs, where sensor nodes are often deployed in remote or inaccessible locations, making battery replacement difficult or impractical. The limited energy resources of these nodes pose a significant constraint on their operational lifespan and the overall sustainability of IoT networks.[1, 2, 3, 5, 4]

To address this challenge, a significant body of research is focused on developing energy-efficient solutions for IoT networks, with a particular emphasis on WSNs. The research papers in your Google Drive delve into this area, exploring various approaches to optimize energy consumption and extend the operational lifespan of these networks. These approaches include Energy-aware routing protocol, Efficient clustering algorithms, Energy harvesting techniques, Sleep mode and duty cycling strategies

These research efforts collectively contribute to building a greener and more sustainable IoT ecosystem. By addressing the crucial challenge of energy efficiency, they pave the way for the widespread deployment and adoption of IoT technologies, unlocking their full potential to transform our world while minimizing their environmental impact. The research findings presented in these papers provide valuable insights into the design and implementation of energy-efficient WSNs, contributing to the advancement of IoT technology and its sustainable integration into various aspects of our lives.

2|Literature Review

The paper "Data Security and Privacy in the IoT" by Elisa Bertino discusses the challenges of securing IoT systems due to their large scale, device heterogeneity, and dynamic environments. Traditional security techniques, like encryption and access control, are often difficult to apply in IoT because of limited device resources and inconsistent implementation. IoT systems also introduce significant privacy concerns, especially when handling sensitive data, such as health information. The paper highlights the need for research into scalable encryption methods, protection mechanisms for small devices, and ensuring data integrity and quality in IoT environments[1].The paper "Security, Privacy, and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey" explores the security, privacy, and trust issues within the Mobile Internet of Things (M-IoT). M-IoT expands on traditional IoT by introducing mobile, connected, and low-complexity devices. While M-IoT enables innovative applications in sectors such as healthcare, smart cities, and industrial monitoring, it faces significant challenges in maintaining secure and trustworthy communication. The survey outlines current solutions, including secure protocols, trust management, and privacy-preserving techniques, and highlights the need for future research to improve the resilience of M-IoT systems against evolving threats[2].The paper "Scalability in Internet of Things: Techniques, Challenges and Solutions" explores the concept of scalability in IoT, which is crucial as the number of connected devices increases. Scalability ensures that a system can handle growth by adapting to environmental and user needs. The paper explains two types of scalability: vertical scalability, which enhances system capacity by adding resources like memory or processing power, and horizontal scalability, which improves performance by adding more instances to reduce server load. The paper also discusses challenges like latency, packet loss, and design constraints, and offers solutions such as edge computing and distributed architectures to improve scalability and reduce costs[3].The document discusses the Internet of Things (IoT), emphasizing its increasing role in creating a connected, intelligent digital environment. It highlights how IoT is transforming industries by integrating physical and digital components, enhancing efficiency, productivity, and innovation. The paper explores IoT architecture, technologies, components, and applications, focusing on smart home automation that enables remote control of household devices. Additionally, it outlines the exponential growth of IoT, its characteristics, major components, and the communication technologies involved. Finally, it addresses key IoT security challenges and risks, recommending solutions to safeguard privacy and data integrity[4].The paper presents a system to enhance the security and efficiency of data transmission between IoT devices and the cloud. It proposes using a fog computing layer between IoT and the cloud to filter, clean, and classify data before sending it to the cloud. This reduces network traffic, decreases server load, and ensures data integrity. Techniques such as K-nearest neighbor (KNN) and complement naive Bayes (CNB) are used for data filtering. By processing data at the fog level, the system improves security, lowers latency, and enhances the performance of IoT applications[5].The paper focuses on improving security in IoT networks, particularly in key exchange, user authentication, and data integrity. It presents a framework utilizing a Gateway Node (GWN) for secure connections and key generation, emphasizing energy efficiency and reduced computation time. The study proposes a Compressed Trie-based Group Key Distribution (CTGKD) protocol for scalable

and secure key management, improving communication while maintaining system integrity. The framework addresses challenges in IoT security, ensuring secure data transmission and enhancing user authentication and session key generation, critical for industrial and cloud environments[6].The paper discusses data transmission in IoT networks, focusing on the integration of 5G technology. It highlights the challenges and benefits of IoT, emphasizing secure and efficient data transfer with accuracy, integrity, and low latency. The paper explores the components needed for IoT implementation, such as sensors and communication protocols, and introduces concepts like network slicing in 5G for improved quality of service. It also covers technical aspects, such as protocol signaling, PDU session establishment, and UE configuration, and outlines challenges in network operations while stressing the future importance of network slicing in 5G systems[7].The paper titled "Secure and Scalable IoT: An IoT Network Platform Based on Network Overlay and MAC Security" by Junwon Lee and Heejo Lee focuses on improving the security and scalability of IoT networks. The authors highlight the vulnerabilities and security threats present in IoT environments, such as MITM attacks, DNS manipulation, and data tampering. To address these challenges, the paper introduces a new IoT-specific network security platform (SSI) that minimizes the use of computing resources on IoT devices. The platform leverages Layer 2 tunneling protocols (L2TP and VXLAN) for scalability and applies the MACsec encryption protocol to secure data frames. In comparison to traditional TCP/IP-based VPNs, the proposed system demonstrates better performance, improving network speed by 30% and reducing CPU usage by 31.6%[8].The paper discusses secure data communication within the Internet of Things (IoT) landscape. It highlights the current challenge of interoperability due to varying proprietary protocols and communication hardware from different manufacturers. The paper proposes a virtual network testbed for smart home IoT frameworks, integrating components from various architecture proposals. It aims to provide a common framework for IoT device interaction, emphasizing secure data transfer, protocol efficiency, and scalability. The study also demonstrates the development of simulations for IoT devices, offering a practical method to test IoT frameworks without the need for physical hardware[9].The paper "Secure and Efficient Data Transmission in Internet of Things (IoT) Networks: A Review of Protocols and Techniques" provides a comprehensive analysis of the challenges in IoT security and explores various protocols, encryption methods, and authentication mechanisms to address these issues. The authors emphasize the importance of securing data transmission through end-to-end encryption, access control, and secure bootstrapping. The review also covers emerging technologies such as blockchain, machine learning for anomaly detection, and post-quantum cryptography, while proposing future research directions to combat evolving security threats in IoT networks[10].The paper presents a scalable and secure architecture for distributed IoT systems by integrating blockchain and artificial intelligence (AI) technologies. It addresses the vulnerabilities of traditional centralized IoT systems, which are susceptible to cyber-attacks and data breaches. The proposed solution uses a permissioned blockchain to enhance security, decentralize control, and manage IoT data securely. Additionally, AI modules at the network's edge detect and classify malware in real time using machine learning algorithms like decision trees and neural networks. The architecture was tested through simulations, demonstrating high efficiency in detecting and mitigating cyber threats[11].The document discusses the concept of scalability in the Internet of Things (IoT), focusing on its importance, features, techniques, and associated research challenges. Scalability is the ability of a system to handle growth effectively, making it crucial for IoT systems due to the rapidly increasing number of connected devices. The paper differentiates between vertical scalability (enhancing existing resources) and horizontal scalability (adding new hardware or software units). It also highlights various features needed for scalability, including business, marketing, hardware, software, and network considerations. Techniques such as automated bootstrapping, microservices architecture, and controlling data pipelines are explored. Lastly, the document identifies challenges such as protocol security, identity management, privacy, trust, and fault tolerance as key issues in achieving scalable IoT systems[12].The document presents a research study focused on developing encryption standards for enhancing information security at the Internet of Things (IoT) network layer, particularly in the transport layer. As IoT devices proliferate, ensuring secure transmission of vast data has become critical, necessitating enhanced security measures. The study proposes a new security strategy tailored for the IoT transport layer, which is designed to improve data confidentiality and integrity while addressing issues like high resource consumption and adaptability to various network topologies. Through simulations and experiments, the proposed strategy shows promising results in enhancing security and efficiency, particularly in resource-constrained environments. The findings underscore the importance of continually refining security protocols to meet evolving threats and technological advancements in IoT networks[13].The paper proposes a scalable and secure Big Data IoT system, integrating cloud computing with multifactor authentication and lightweight cryptography. It focuses on protecting sensitive and nonsensitive data by dividing them between private and public clouds, respectively. Sensitive data is encrypted using RC6 and Fiestel encryption algorithms, while nonsensitive data is secured with AES encryption. A multilevel authentication system ensures data security, with levels depending on the data's sensitivity and user access requirements. The system is tested for computational efficiency, security strength, and encryption/decryption times, demonstrating improved performance over existing methods[14].The document discusses the design of a secure and scalable service agent for IoT transmission using a fusion of blockchain technology and the

MQTT communication protocol. With the rapid development of IoT, data security during transmission has become a major concern. The study improves message transmission by integrating blockchain with MQTT, eliminating the need for centralized control, and enhancing encryption for better security and flexibility. It proposes a new encryption mode and system architecture that ensures data integrity and prevents tampering. Through experiments, the method demonstrates improved security and reduced technical challenges in IoT communication[15].The paper presents a deep learning-based method for secure data transmission in IoT systems using cloud computing, employing Generative Adversarial Networks (GANs). It compares the GAN model's performance on the UNSW-NB15 dataset against other machine learning techniques like decision trees and random forests. The GANs approach, which integrates LSTM and CNN, achieved high accuracy (98.07%), precision (98.45%), and an AUC-ROC score of 0.998, outperforming traditional models in predicting secure data transmission. This method enhances security in IoT networks by predicting data encryption during transmission[16].The document outlines a secure transmission technique for data in IoT edge computing infrastructure, particularly focusing on smart city applications. It addresses challenges like privacy, security, and the risks posed by open communication mediums used by IoT devices. The proposed method involves three phases: registration, authentication, and data transfer, using Euclidean parameters to enhance security. This technique helps IoT sensors authenticate and communicate securely with readers and base stations, protecting against common attacks such as authentication and replay attacks, while improving the reliability of smart city infrastructure[17].The paper titled "Scalable and Secure Internet of Things Connectivity" explores the challenges of scalability and security in IoT environments, particularly with the use of blockchain technology. It presents a framework for enhancing security and scalability by using blockchain-based authentication and whitelisting techniques. The authors analyze traditional IoT authentication methods and propose a blockchain-integrated system where security is automatically evaluated and enforced. The proposed model reduces the vulnerabilities of IoT devices and ensures secure connectivity and extension by penalizing insecure devices while rewarding secure ones. This system was tested in a simulation, showing improved security and scalability compared to traditional methods[18].The document presents LogSafe, a secure and scalable data logger designed for IoT devices, addressing privacy and security concerns in IoT environments. With the increasing use of IoT, significant personal data is generated, which can be vulnerable to cyber-attacks. LogSafe leverages Intel's Software Guard Extensions (SGX) to securely store logs from IoT devices on untrusted cloud infrastructures. It ensures the Confidentiality, Integrity, and Availability (CIA) of IoT data by using encryption, secure hashing, and a fault-tolerant architecture. The system is scalable, capable of handling numerous devices, and supports forensic analysis to detect potential security breaches. Through evaluations, LogSafe demonstrates efficiency, handling high data rates without compromising security, although there are challenges such as computational overhead, which are mitigated through design optimizations[19].The document "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications" presents a framework to enhance secure healthcare data transmission in IoT environments. The proposed system utilizes optimized routing protocols, including the fuzzy dynamic trust-based RPL (FDT-RPL) and butter ant optimization algorithm (BAO), to improve security, reduce energy consumption, and ensure scalability. The framework integrates data preprocessing techniques such as K-nearest neighbor imputation and principal component analysis (PCA) for efficient data handling. The results demonstrate improved performance in terms of data transmission security, network lifetime, and reduced packet loss, making the system suitable for mobile healthcare applications[20].The document titled *"Data Protection Mechanisms in IoT: A Vital Challenge"* focuses on the growing threats to privacy and security in the Internet of Things (IoT) due to the interconnected nature of devices. It reviews various security challenges like access control, authentication, data encryption, and trust management in IoT systems. The paper analyzes existing security frameworks, lightweight cryptographic solutions, and key management techniques, discussing their advantages and limitations. It emphasizes the need for adaptable, scalable security models that balance efficiency with the resource limitations of IoT devices while addressing emerging attack vectors like denial-of-service, eavesdropping, and unauthorized data access[21].The paper "Secure Data Transmission with Neural Network Cluster for IoT Applications" proposes a Device-to-Device Mobile Edge Computing (D2D-MEC) system to improve computational capacity and security in IoT environments. The system uses neural network clustering for node selection, focusing on reducing edge computation resources and maximizing the number of devices supported. The paper also introduces location-based key management to enhance data transmission security. The method, tested using the NS2 simulator, demonstrates improvements in packet delivery, reduced energy consumption, and secured communication in mobile IoT networks[22].The paper discusses a controllable privacy data transmission mechanism for IoT systems using blockchain technology. The authors propose a framework that ensures data reliability, traceability, and security in IoT environments, addressing issues like chaotic data circulation and data accountability. By using smart contracts and cryptographic techniques within a consortium blockchain structure, the system facilitates decentralized, secure, and scalable data exchanges between IoT devices. A prototype system built on Hyperledger Fabric is presented, demonstrating the mechanism's effectiveness in ensuring trusted, traceable data transmission with privacy protection[23].The paper titled "Internet of Things (IoT) for Next-Generation

Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios" provides an extensive overview of IoT's role in the upcoming 5G network landscape. It outlines the current challenges, use cases, and technological trends for integrating IoT with 5G. Key enablers such as MIMO, CRAN, and NFV are discussed, alongside issues like security, scalability, and energy efficiency. The paper also explores the role of AI in enhancing IoT applications and the challenges of massive device connectivity and QoS standards for future 5G-IoT systems[24].The paper titled *"Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography" proposes a secure cloud-based IoT architecture to address security challenges in managing and storing big data. The architecture leverages multifactor authentication (MFA) and lightweight cryptographic methods (RC6, Fiestel, and AES) for encrypting sensitive and nonsensitive data, respectively. A hybrid cloud model is employed to store sensitive data in private clouds and nonsensitive data in public clouds. The system is evaluated for its computational efficiency, encryption and decryption time, and security strength. The results indicate that the proposed system outperforms existing methods in these areas[25].

3 | Methodology

3.1 | Comprehensive Needs Assessment

3.1.1 | Detailed Problem Identification:

Specific Challenges:
Clearly identify the unique energy-efficiency challenges faced by your IoT or WSN application, such as high data rates, long transmission ranges, real-time requirements, or environmental factors [8].

Root Causes:
Analyze the underlying causes of these challenges to identify potential areas for improvement. For example, if high data rates are a concern, explore ways to reduce data redundancy or optimize communication protocols [8].

3.1.2 | Prioritization of KPIs

Application-Specific Goals:
Determine the most critical KPIs based on the specific goals and requirements of your application. For instance, if network lifetime is paramount, prioritize energy consumption per node and duty cycling [8].

Trade-offs
Consider the trade-offs between different KPIs. For example, increasing throughput may require higher transmission power, which can lead to increased energy consumption [7].

Constraint Analysis:

-Hardware Limitations: Identify the limitations of your hardware resources, such as battery capacity, processing power, and memory [1].

-Network Topology: Analyze the impact of your network topology on energy consumption. For example, a star topology may require longer transmission distances and higher power consumption compared to a mesh topology [1].

-Data Transmission Requirements: Assess the volume, frequency, and sensitivity of data transmissions to determine the optimal energy-efficient strategies [2].

3.2 | Tailored Network Architecture and Topology

3.2.1 |Hybrid Clustering Approaches:

Combining Strengths:
Explore hybrid clustering techniques that combine the advantages of different algorithms, such as LEACH and DEEC. For example, LEACH can be used for initial clustering, while DEEC can be used to adapt to changes in node density [9].

Dynamic Adaptation:
Implement mechanisms that allow the clustering algorithm to dynamically adapt to changing network conditions, such as node failures or variations in data traffic [9].

3.2.2 |Intelligent Sink:

Optimization Algorithm Utilize optimization algorithms to determine the optimal placement of mobile sinks or base stations based on factors like node density, energy levels, and data transmission patterns [9].

Mobility Patterns
Consider the mobility patterns of nodes and sinks to ensure efficient data collection and transmission [9].

3.2.3 | Hierarchical Routing with Energy Balancing:

Energy-Aware Routing:
Implement routing protocols that consider the residual energy of nodes when selecting routes [9]

Energy Balancing Mechanisms:
Incorporate mechanisms that distribute energy consumption evenly among nodes, preventing premature failure of high-energy nodes [9].

3.3 | Advanced Communication Protocols:

3.3.1 | Adaptive Duty Cycling:

Dynamic Adjustment:
Implement mechanisms that dynamically adjust wake-up intervals based on network conditions, such as data traffic, node energy levels, and environmental factors [4].

Event-Driven Wake-ups:
Explore event-driven wake-ups to minimize energy consumption by allowing nodes to sleep until triggered by specific events [21].

3.3.2 | Energy-Aware Routing with Data Aggregation:

In-Network Aggregation:

Optimize routing protocols to prioritize data aggregation opportunities, reducing redundant transmissions and conserving energy [5].

Data Fusion:
Implement data fusion techniques to combine data from multiple sensors to extract relevant information while minimizing transmission overhead [5].

3.3.3| Cooperative Communication:

Relaying:
Explore relaying techniques where nodes can assist each other in transmitting data, reducing transmission distances and power consumption [5].

Cooperative Diversity:
Implement cooperative diversity techniques to improve transmission reliability and reduce energy consumption by combining signals from multiple nodes [5].

3.4 |Innovative Energy Harvesting and Management

3.4.1 | Multi-source Energy Harvesting:

Hybrid Approaches:
Consider combining multiple energy harvesting techniques, such as solar, RF, and vibration, to maximize energy availability and resilience [17] .

Energy Storage:
Explore efficient energy storage solutions, such as batteries or supercapacitors, to store harvested energy for later use [17].

3.4.2 | Intelligent Energy Allocation:

Priority-Based Allocation:
Develop algorithms that allocate harvested energy to tasks based on their priorities and energy requirements [17].

Dynamic Adjustment:
Implement mechanisms that dynamically adjust energy allocation based on changing network conditions and application demands [17].

3.4.3 | Energy-Aware Scheduling:

Task Prioritization:
Prioritize tasks based on their importance and energy consumption requirements [17] .

Scheduling Optimization:
Develop scheduling algorithms that minimize energy consumption while meeting application deadlines [17].

3.5 | Holistic Performance Evaluation

3.5.1 | Simulation with Real-World Data:

Realistic Scenarios:
Use simulation tools with real-world data sets to evaluate the performance of proposed solutions under realistic conditions [11].

Scenario-Based Analysis:
Consider different scenarios, such as varying node densities, data traffic patterns, and environmental conditions, to assess the robustness of your solutions [11].

3.5.2 | Experimental Validation:

Controlled Environments:
Conduct controlled experiments in laboratory settings to validate simulation results and identify any unforeseen challenges [11].

Real-World Deployments:
Deploy your solutions in real-world environments to assess their performance under actual operating conditions [11].

3.5.3 | Iterative Refinement:

Continuous Improvement:
Continuously refine your methodology based on evaluation results and emerging trends in IoT and WSN technologies [11].

Feedback Loop:
Establish a feedback loop between evaluation and design to identify areas for improvement and make necessary adjustments [11].

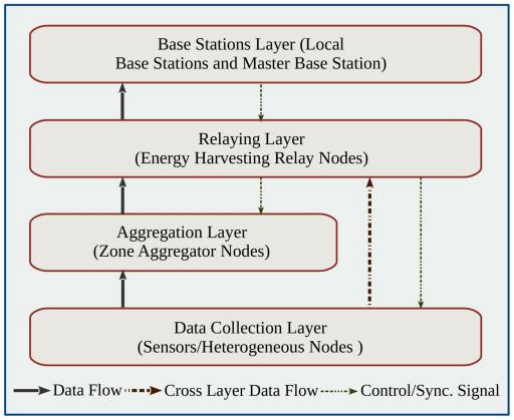


Figure 1: architecture of the network model [1].

By following this refined methodology and incorporating the latest advancements in IoT and WSN technologies, you can develop highly energy-efficient solutions that meet the demanding requirements of modern applications while ensuring sustainability and long-term viability.

6 | Proposed Work

The research papers provide a comprehensive overview of the challenges and solutions related to energy efficiency in Internet of Things (IoT) and Wireless Sensor Networks (WSNs). A key trend emerging is the recognition of energy efficiency as a critical constraint in IoT and WSN deployments. The limited battery capacity of sensor nodes significantly impacts network lifetime, communication range, and overall performance.

To address this challenge, researchers have explored various techniques, including clustering, data aggregation, routing protocols, duty cycling, and energy harvesting. Clustering algorithms, such as LEACH and its variants, organize nodes into clusters to reduce transmission overhead and conserve energy. Data aggregation methods, like in-network aggregation and sensor data fusion, further optimize energy consumption by reducing the amount of data transmitted. Energy-aware routing protocols consider factors such as residual energy, distance to the sink, and link quality to select energy-efficient routes.

Duty cycling and sleep modes are widely adopted to minimize energy consumption during idle periods. Adaptive duty cycling allows nodes to adjust their sleep-wake schedules based on network conditions and application requirements. Energy harvesting techniques, such as solar, RF, and vibration energy harvesting, offer promising solutions for supplementing battery power and extending network lifetime.

Heterogeneous networks, where nodes have different energy capabilities and functionalities, are gaining attention as a means to optimize energy consumption. These networks allow for efficient task allocation and energy distribution, ensuring that nodes with higher energy reserves can take on more demanding tasks.

While energy efficiency is paramount, the research papers also emphasize the importance of network security and Quality of Service (QoS). Security measures, such as encryption and authentication, are essential to protect sensitive data transmitted over IoT and WSN networks. However, these measures can introduce additional computational overhead and energy consumption. Ensuring acceptable levels of QoS, such as low latency and high reliability, may also require higher energy consumption.

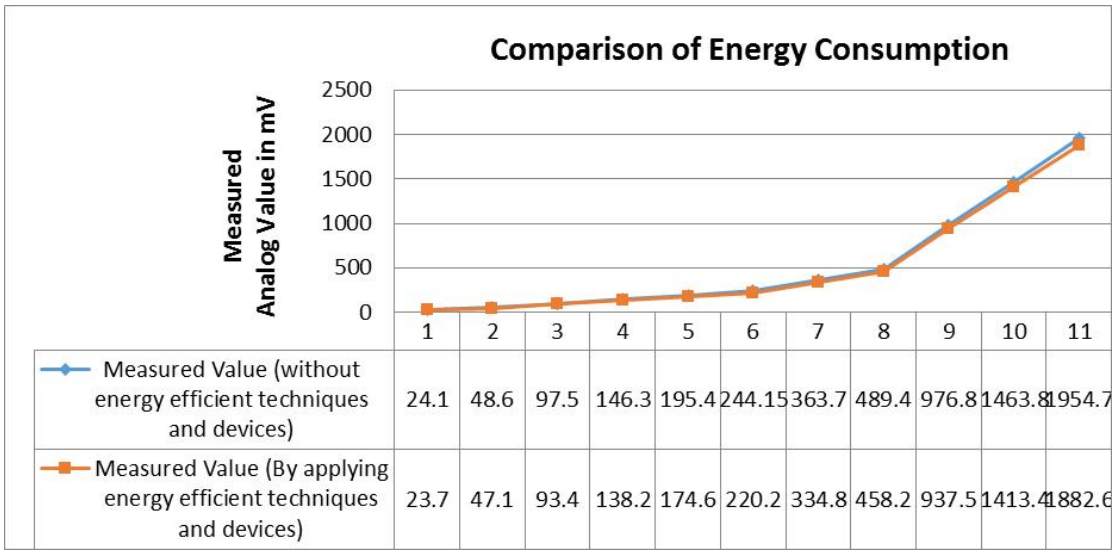
The researchers rely heavily on simulation tools, such as NS-3 and OMNeT++, to evaluate the performance of proposed energy-efficient solutions. Experimental validation in controlled environments or real-world deployments is also crucial for confirming simulation results and assessing real-world applicability.

In conclusion, the research papers provide valuable insights into the challenges and solutions related to energy efficiency in IoT and WSNs. By understanding these trends and incorporating the latest advancements in technology, researchers and practitioners can develop more effective energy-efficient solutions that address the limitations of battery-powered sensor nodes and ensure the long-term sustainability of IoT and WSN deployment.

Distance in cm	Measured Analog Value in mV (without energy efficient techniques and devices)	Measured Analog Value in mV (By applying energy efficient techniques and devices)	Difference in energy consumption
5	24.1	23.7	0.4
10	48.6	47.1	1.5
20	97.5	93.4	4.1
30	146.3	138.2	8.1
40	195.4	174.6	20.8
50	244.15	220.2	23.95
70	363.7	334.8	28.9
100	489.4	458.2	31.2
200	976.8	937.5	39.3
300	1463.8	1413.4	50.4
400	1954.7	1882.6	72.1

Table 1: Comparing power consumption with and without using any energy efficient techniques [21]

The comparison graph is shown in Figure 2 as below



2: Graph showing comparison of power consumption with and without using any energy efficient techniques [21]

Measure the effectiveness of anomaly detection algorithms in identifying and preventing unauthorized access or cyberattacks.

5 | Results and Discussion

RESULT:

The study on energy-efficient protocols for IoT devices, particularly within Wireless Sensor Networks (WSNs), provides a detailed assessment of various methodologies to mitigate the energy challenges inherent in these networks. Key results demonstrate that clustering algorithms like LEACH (Low-Energy Adaptive Clustering Hierarchy) and DEEC (Distributed Energy-Efficient Clustering) significantly reduce energy consumption by grouping sensor nodes into clusters, which minimizes redundant data transmission. This clustering approach allows nodes to conserve energy by reducing their need for direct communication with distant base stations.

Energy-aware routing protocols also show promising results by selecting paths based on the residual energy levels of nodes and the efficiency of the transmission path. By implementing adaptive routing that accounts for energy levels, the network prevents nodes with lower energy from overuse, which reduces the frequency of node failure and enhances network longevity. Data aggregation and in-network fusion techniques, such as data fusion and cooperative communication, further optimize network energy usage by reducing the volume of transmitted data. These methods ensure that only relevant information reaches the base station, reducing the energy cost per transmission and enhancing the network's efficiency.

Moreover, the implementation of sleep mode technologies and adaptive duty cycling has led to substantial improvements in energy conservation. These techniques allow nodes to remain in low-energy states during idle periods, waking only when necessary, which reduces overall energy consumption without compromising data availability. Energy harvesting strategies—especially solar and radio frequency (RF) harvesting—have also shown positive results by supplementing battery power, extending node lifespan, and reducing dependence on external energy sources. Simulation tools like NS-3 and OMNeT++ used in experimental setups validate these findings, with metrics showing increased network lifetime, reduced power consumption, and more efficient energy allocation.

DISCUSSION:

The findings emphasize the importance of energy-efficient protocols in the sustainable development of IoT systems. The rapid growth of IoT networks, often constrained by battery-operated devices deployed in inaccessible locations, presents a significant challenge to network longevity and environmental sustainability. Clustering algorithms and energy-aware routing protocols provide a foundational solution, addressing these issues by organizing nodes into clusters and optimizing transmission routes based on residual energy levels. The reduction of direct, high-energy transmissions extends the overall network lifespan and ensures more reliable data flow even in energy-limited scenarios.

However, while these protocols address many challenges, the study also highlights limitations and areas for further research. For instance, there are trade-offs between energy efficiency and Quality of Service (QoS) requirements, such as low latency and high data reliability. Protocols that emphasize energy conservation may introduce delays in data transmission or reduced reliability, which could affect applications that require real-time responses, such as healthcare monitoring or industrial automation. Balancing these trade-offs remains a critical research area to ensure that IoT networks can provide both energy efficiency and robust service.

The research also suggests that future advancements in machine learning (ML) and artificial intelligence (AI) could further improve the adaptability of IoT protocols. AI-driven approaches could dynamically adjust network parameters, such as sleep and wake cycles, based on real-time data patterns and environmental conditions, thus optimizing energy use. For example, machine learning algorithms could predict periods of low data activity, enabling nodes to enter sleep mode more effectively without impacting data transmission. Predictive analytics could also be used to forecast potential node failures, allowing for proactive maintenance and reducing downtime.

Another promising area for development is the integration of multi-source energy harvesting, where IoT nodes leverage multiple energy sources—such as solar, RF, and kinetic energy—depending on their environment. This diversification in energy sources would enhance the reliability of energy-harvesting methods and contribute to self-sustaining IoT networks. Future studies could focus on optimizing the switching between energy sources based on availability, efficiency, and environmental conditions to further improve IoT node autonomy.

While the research presents a solid foundation, it also reveals the importance of practical deployment and real-world validation. Many protocols and techniques tested in simulated environments may face challenges when implemented on a large scale in diverse settings like smart cities, agriculture, or environmental monitoring. Therefore, real-world deployment is critical to fully assess protocol efficacy, with additional focus on scalability, security, and interoperability with other IoT systems.

In conclusion, the study provides a comprehensive analysis of energy-efficient protocols for IoT devices, offering several promising solutions to address the critical issue of energy consumption. By implementing clustering, energy-aware routing, adaptive duty cycling, and energy harvesting techniques, IoT networks can significantly reduce power usage, thereby enhancing device lifespan and promoting sustainable deployment. Future research should focus on balancing energy efficiency with performance requirements, integrating AI for predictive energy management, and validating protocols in real-world settings to ensure applicability. These advancements will be essential for enabling the widespread, sustainable adoption of IoT in various sectors, ensuring that IoT networks can continue to grow and benefit society while minimizing environmental impact.

6 | Future Works

The future of energy-efficient IoT, particularly WSNs, holds immense promise. Based on the research explored, several key trends are emerging:

6.1 | Extended Network Lifespans

6.1.1 | Energy-Aware Routing:

By intelligently selecting routes that minimize energy consumption, WSNs can operate for longer periods without battery replacements.

6.1.2 |Efficient Clustering:

Grouping sensor nodes into clusters to reduce redundant data transmissions can significantly extend network lifespan.

6.2 | Self-Powered WSNs

6.2.1 | Energy Harvesting:

By harnessing energy from the environment (e.g., solar, thermal, vibration), WSNs can become self-sufficient, reducing reliance on batteries and enabling long-term deployments.

6.3 | AI and Machine Learning Integration

6.3.1 |Intelligent Optimization :

AI algorithms can analyze network data and dynamically adjust parameters to optimize energy consumption in real-time.

6.3.2 | Predictive Maintenance:

AI can predict potential failures and schedule maintenance tasks proactively, reducing energy wastage.

6.4 | AI and Machine Learning Integration

6.4.1 | Reliable Communication:
Energy-efficient protocols can improve data transmission reliability and reduce packet loss

6.5 | Wider Adoption of IoT Applications

6.5.1 | Smart Cities :
Energy-efficient WSNs can enable intelligent city management, optimizing resource usage and improving urban living**.**

6.5.2 | Precision Agriculture:
WSNs can monitor soil moisture, temperature, and other environmental factors to optimize irrigation and fertilization, leading to increased crop yields and reduced water usage.

6.5.3 | Industrial Automation:
WSNs can monitor equipment health and optimize production processes, leading to increased efficiency and reduced energy consumption.

6.6 | Greener and More Sustainable IoT

6.6.1 | Reduced Environmental Impact:
By minimizing energy consumption and reducing the need for battery replacements, energy-efficient WSNs contribute to a more sustainable future.

6.7 | Standardization and Interoperability

6.7.1 | Reduced Environmental Impact:
The development of standardized protocols will enable seamless integration of devices from different manufacturers, fostering innovation and reducing implementation costs.

In conclusion, the future of energy-efficient IoT is bright. By addressing the challenges of energy consumption and leveraging advancements in technology, we can create a more sustainable and interconnected world

7 | Conclusion

The future of energy-efficient IoT, particularly WSNs, is poised for significant growth and innovation. By addressing the critical challenge of energy consumption, researchers and engineers are paving the way for a more sustainable and interconnected world. The integration of AI and machine learning, along with advancements in energy harvesting and low-power technologies, will further enhance the capabilities and longevity of IoT devices. As WSNs become more energy-efficient and reliable, they will find applications in a wide range of domains, from smart cities and agriculture to healthcare and environmental monitoring. By embracing energy efficiency as a core principle, we can unlock the full potential of the IoT and create a brighter future for all.

Acknowledgments

I would like to express my heartfelt gratitude to **Dr. Hitesh Mahapatra** for his invaluable guidance and support throughout our research on .IoT-Based Smart City Grid Optimization Using AI and Edge Computing .. His deep knowledge, constructive feedback, and dedication have been instrumental in shaping the direction and quality of this work. Dr. Mahapatra's mentorship has not only enhanced my understanding of cutting-edge technologies but also encouraged me to think critically and innovatively. I am deeply appreciative of his encouragement and contributions, which have significantly enriched my research experience. Thank you for being an inspiring mentor.

Author Contributaion

Neelu Kumari, Parul Kumari, Saket Kumar: Conceptualization and Design, Literature Review, Methodology and Analysis, Results and Discussion, conclusion and future research.

Funding

This research received no external funding **.**

Data Availability

The data used and analyzed during the current study are available from the corresponding author upon reasonable request

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.These sections should be tailored to reflect the specific details and contributions if necessary.

References

[1] Rahamathunnisa, U., Vivekanand, C. V., Chithras, T., Sreedevi, E., Kiran, V., & Rajendiran, M. (2024). Energy-efficient communication protocols for IoT devices. 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), 1-8. IEEE.

[2] Venčkauskas, A., Jusas, N., Kazanavicius, E., & Stuikys, V. (2015). An energy-efficient protocol for the Internet of Things. Journal of Electrical Engineering, 66(1), 7-12.

[3] Hemanand, D., Ambika, C., Bhuvaneswari, S., Savitha, S., Jothi, M., & Rama, R. S. (2024). Optimizing energy-efficient communication protocols for IoT devices in smart cities using Narrowband IoT and LTE-M technology. J. Electrical Systems, 20(5s), 2149-2157.

[4] Abdul-Qawy, A. S. H., Alduais, N. A. M., Saad, A.-M. H. Y., Taher, M. A. A., Nasser, A. B., Saleh, S. A. M., & Khatri, N. (2023). An enhanced energy efficient protocol for large-scale IoT-based heterogeneous WSNs. Scientific African, 21, e01807.

[5] Venčkauskas, A., Jusas, N., Kazanavicius, E., & Stuikys, V. (2015). An energy efficient protocol for the Internet of Things. Journal of Electrical Engineering, 66(1), 47-52.

[6] Safara, F., Souri, A., Baker, T., Al Ridhawi, I., & Aloqaily, M. (2020). PriNergy: A priority-based energy-efficient routing method for IoT systems. Journal of Supercomputing.

[7] Khan, S. B., Kumar, A., Mashat, A., Pruthviraja, D., Rahmani, M. K. I., & Mathew, J. (2024). Artificial Intelligence in Next-Generation Networking: Energy Efficiency Optimization in IoT Networks Using Hybrid LEACH Protocol. SN Computer Science, 5(546).

[8] Farhan, L., Hameed, R. S., Ahmed, A. S., Fadel, A. H., Gheth, W., Alzubaidi, L., Fadhel, M. A., & Al-Amidie, M. (2021). Energy efficiency for green Internet of Things (IoT) networks: A survey. Network, 1(3), 279-314.

[9] Dogra, R., Rani, S., Babbar, H., & Krah, D. (2022). Energy-Efficient Routing Protocol for Next-Generation Application in the Internet of Things and Wireless Sensor Networks. Wireless Communications and Mobile Computing, 2022, Article ID 8006751.

[10] Gray, C., Campbell, L., Ayre, R., & Hinton, K. (2019). Energy-efficient network protocols for domestic IoT application design. Journal of Telecommunications and the Digital Economy, 7(2), Article 184.

[11] Abbas, M. T. (2023). Improving the energy efficiency of cellular IoT devices (Licentiate thesis, Karlstad University). Karlstad University Studies, 2023:8. ISBN 978-91-7867-351
[12] Reddy, P. K., & Babu, R. (2017). An evolutionary secure energy efficient routing protocol in Internet of Things. International Journal of Intelligent Engineering and Systems, 10(3), 337-346.
[13] Vashishth, V., Chhabra, A., Khanna, A., Sharma, D. K., & Singh, J. (2019). An energy efficient routing protocol for wireless Internet-of-Things sensor networks. arXiv, 1808.01039.
[14] Safara, F., Souri, A., Baker, T., Al Ridhawi, I., & Aloqaily, M. (2020). PriNergy: A priority-based energy efficient routing method for IoT systems. Journal of Supercomputing.
[15] Duy Tan, N., Nguyen, D.-N., Hoang, H.-N., & Le, T.-T.-H. (2023). EEGT: Energy efficient grid-based routing protocol in wireless sensor networks for IoT applications. Computers, 12(5), 103.
[16] Deokar, R. D. (2023). Design and analysis of energy efficient routing protocols for IoT devices [Doctoral research proposal, Swami Ramanand Teerth Marathwada University].
[17] Dogra, R., Rani, S., & Gianini, G. (2023). REERP: A region-based energy-efficient routing protocol for IoT wireless sensor networks. Energies, 16(6248).
[18] Malla, S., Sahu, P. K., Patnaik, S., & Nayak, M. (2023). Smart energy efficient techniques for IoT enabled wireless node. Journal of Theoretical and Applied Information Technology, 101(18), 7331-7346.
[19] Behera, T. M., Samal, U. C., & Mohapatra, S. K. (2018). Energy-efficient modified LEACH protocol for IoT application. IET Wireless Sensor Systems, 8(5), 223-228.
[20] Tan, N. D., Nguyen, D.-N., Hoang, H.-N., & Le, T.-T.-H. (2023). EEGT: Energy efficient grid-based routing protocol in wireless sensor networks for IoT applications. Computers, 12(5), 103.
[21] Malla, S., Sahu, P. K., Patnaik, S., & Nayak, M. (2023). Smart energy efficient techniques for IoT enabled wireless node. Journal of Theoretical and Applied Information Technology, 101(18), 7331-7346.
[22] Lohiya, H., & Kasliwal, S. (2022). Enhancing the energy efficiency of IoT for 5G technology. International Journal of Food and Nutritional Sciences, 11(12), 2551-2561.
[23] Venčkauskas, A., Jusas, N., Kazanavičius, E., & Štuikys, V. (2015). An energy efficient protocol for the Internet of Things. Journal of Electrical Engineering, 66(1), 47-52.
[24] Sheikh, A. M., & Joshi, S. (2024). Energy efficient MIMO-based IoT networks: An overview. Journal of EmergingTechnologies and Innovative Research (JETIR), 11(1), 63-68.