A Systematic Review of Energy-Efficient Routing Protocols for IoT Networks

Samuel BoahAkenten Appiah-Menka
University of Skills Training and Entrepreneurial Development (AAMUSTED)
Cecilia Ampofowaa
Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED)
William Asiedu
Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED)
Franco Osei-Wusu
fosei-wusu@aamusted.edu.gh

Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED)

Systematic Review

Keywords: Routing Protocol, Energy Efficiency, Wireless Sensor Networks (WSNs), Internet of Things (IoT), Network Lifetime, Data Transmission

Posted Date: October 16th, 2025

DOI: https://doi.org/10.21203/rs.3.rs-7611247/v1

Additional Declarations: No competing interests reported.

Abstract

With the proliferation of the Internet of Things (IoT) in areas like healthcare, smart cities, and industrial automation systems, one herculean task that has been looming and must be addressed is the need to ensure that data transmission is energy-efficient because all IoT devices have limited resources. This article is a systematic literature review (SLR) of energy-efficient routing mechanisms designed to be used in IoT networks, and it focuses on comparing the energy-efficient routing schemes concerning their energy consumption, latency, and security parameters. The research protocol compiled 32 peer-reviewed scientific articles published between 2017 and 2025, following PRISMA guidelines and with strict inclusion and exclusion criteria. The results reveal that popular protocols like RPL, LEACH, TEEN/APTEEN, or AI-based solutions reflect different trade-offs. The cluster-based and chain-based approaches are known to minimize the energy consumed. In contrast, the hybrid protocols and the AI-based approaches provide trade-offs in optimizing the energy, delay, and security parameters, at the expense of complexity. The review also points out that there is a serious gap in the observance of integrated security mechanisms in numerous energy-oriented protocols. These results indicate that routing techniques that are adaptive and context-sensitive are required to comprehensively treat performance limitations of IoT. Researchers and practitioners who are interested in finding an optimal protocol choice and matching diverse IoT applications can draw important thoughts from the paper.

1. Introduction

Internet of Things (IoT) may be regarded as a system of interconnected devices, which are empowered with sensors, software, and network connections, so they can collect and share data. The IoT has, in recent times, received substantial recognition because of its many implications, such as smart healthcare, home automation, transportation, and smart cities. Recently, Internet devices have been exploited in a variety of applications, such as manufacturing, supply chain, real-time equipment surveillance, environmental preservation, and industrial safety control. However, it is projected that each individual will be connected to the Internet by more than ten devices by 2050 [1]. Nevertheless, such a transition will not be an easy process, as many challenges and problems still have to be addressed in various ways to bring the best out of this technology [2]. In such IoT systems, wireless sensor networks (WSNs) are important to gather smart information required in smart environments [3]. These networks consist of many linked devices that communicate with each other via the internet, and hence, they require the application of energy-efficient routing algorithms to process the data transfer. Energy-efficient routing protocols in Internet of Things (IoT) networks have become a crucial issue to consider, as most devices in IoT networks operate on limited energy sources. Energy efficiency plays an essential role in the IoT to ensure optimal network performance on loosely scattered networks (Magubane et al., 2019). To support data exchange in IoT networks, efficient and reliable routing protocols are necessary to address issues such as bandwidth capacity, energy consumption, and scalability. To support data exchange in IoT networks, efficient and reliable routing protocols are necessary to address issues such as bandwidth capacity, energy consumption, and scalability. The issue of energy efficiency is a major concern in IoT networks, as most sensor nodes will be battery-powered and deployed in inaccessible

locations where it will be cumbersome to replace the batteries regularly. Several reviews on energy-efficient routing protocols for IoT networks have been published in recent years, indicating that this research area is continually evolving with new contributions and constant improvement. Yadav & Kumar (2024) in their study present a survey on energy-efficient routing protocols, aiming to provide a holistic understanding of the state-of-the-art approaches, their characteristics, strengths, limitations, and performance metrics. Their survey encompasses a wide range of energy-efficient routing protocols proposed in the literature, including traditional routing protocols adapted for IoT scenarios and protocols specifically tailored for energy optimization. The study of Suryawanshi (2024) presents a comprehensive analysis of recent advancements in IoT routing techniques and energy-efficient solutions, focusing on multi-objective optimization algorithms such as fractional gravitational search, grey wolf optimization, and hybrid salp swarm-differential evolution algorithms. Additionally, the authors also highlight the critical role of energy-efficient routing in IoT applications, such as smart agriculture, healthcare, and smart cities, emphasizing its importance in prolonging network lifetime and reducing overall operational costs. Bekal et al. (2024) present a review of various energy-efficient routing protocols for wireless sensor networks in their study, comparing standard and enhanced protocols. In addition, the study also discusses trade-offs in energy efficiency, network lifetime, and scalability, providing a comparative table for future researchers to analyze these protocols effectively. Finally, Magubane et al. (2019) evaluate energy-efficient routing protocols for IoT networks, specifically comparing RPL and LOADng. The authors of the study conclude that RPL is the more energy-efficient option, which is crucial for prolonging the operational life of battery-powered IoT devices in constrained environments. Despite the existence of several reviews on energy-efficient routing protocols, a systematic literature review has not been well conducted to facilitate the process of selecting the most suitable energy-efficient routing protocols for different IoT applications. This study aims to address this gap by: (i) To identify and categorize the most frequently used energy-efficient routing protocols in IoT networks. (ii) To evaluate the comparative performance of these protocols in terms of energy consumption, latency, and security. The functionality of the IoT networks depends largely on routing. (iii) To analyze the trade-offs and limitations associated with protocol design and implementation in resource-constrained IoT environments. Proper routing protocols define through which nodes across the network the data packets should reach the target in a central sink or a base-station, and should guarantee the least amount of energy used as well as network lifetime. Therefore, in IoT, energy-efficient routing protocols became the subject of fundamental research. To give a more current, up-to-date view to the reader on the energy-efficient routing protocols for IoT networks, this systematic literature review focuses on studies published between 2017 and 2025.

For this purpose, the remainder of this study is organized as follows: Section 2 provides an overview of the key concept addressed in this study, Section 3 outlines the methodology adopted for conducting the systematic review, Section 4 outlined the results derived from the systematic review, Section 5 presents the discussion, and Section 6 presents the conclusions.

2. Concepts

To better understand the key concept related to energy-efficient routing protocols in IoT networks, this session provides a concise overview of the key concept, laying the groundwork for the systematic review.

2.1 Internet of Things

Internet of Things (IoT) can be understood as a system of interconnected devices, which are empowered with sensors, software, and network connections, so they can collect and share data. These devices, integrated with sensors, actuators, and communication modules, are capable of gathering, transmitting, and processing data in real time [8]. IoT is a rapidly evolving paradigm, envisioned as a network of billions of interconnected devices designed to apply advanced technological solutions to real-world challenges [9].

With the expansion of the Internet, IoT has had an impressive effect on several fields, and there have been numerous IoT applications employed for enhancing the network operation and users' quality of experience [9]. IoT applications can be employed in various areas, including healthcare, industry, cellular networks, smart cities, edge computing, cloud computing, wireless sensor networks (WSNs), software-defined networks (SDNs), and many more.

The architecture of IoT is commonly organized into layers, enabling seamless interaction and communication among diverse devices and systems [8]. The architecture of IoT is divided into 4 different layers, i.e., Sensing Layer, Network Layer, Data Processing Layer, and Application Layer. The architecture of IoT is shown in Fig. 1

2.2 Energy-efficiency

Energy efficiency refers to the approach or strategy that aims at minimizing the amount of energy needed to deliver products and services by utilizing advanced technologies, techniques, or processes that limit energy waste while maintaining or improving performance (energy conservation).

The objective of energy-efficient Internet of Things (IoT) networks is to reduce power usage, thereby extending the lifespan of devices, especially those that are battery-powered or located in remote areas [10].

IoT energy efficiency is created with an architecture that forecasts sensor sleep times guided by battery levels and usage patterns to enable maximum resource usage and maximum energy savings, resulting in the life extension of IoT systems [11].

The energy-efficient architecture for IoT networks consists of layers, namely, sensing and control, information processing, and presentation. The architectural design enables the system to estimate the sensors' sleep duration by considering factors such as their remaining battery power, past usage patterns, and the quality of information needed for a specific application[11].

2.3 Routing Protocol

Routing protocols can be termed as the method that determines how routers share routing information, enabling them to determine routes between any two nodes on a computer network. Routing protocols are guidelines used to determine the optimal path for transferring data among nodes in a network. Through these protocols, communication among routers is established to transmit network packets using the most efficient paths [12].

A routing protocol involves receiving a packet as incoming traffic at an internal node of a distributed router, which contains a global destination address (Yeh et al., 2020).

Many routing protocols have been developed since then, and these protocols differ according to network structure and field of application [13].

There are mainly three kinds of routing protocols applied on the Internet, which are distance vector, link state, and path vector. Every type has basic principles and traits. Also, there are other problems that might be experienced during the temporary occurrence of routing protocols, like looping, and hence, there are different ways of minimizing the occurrence of these problems.

3. Methodology

This paper employs a systematic review methodology to present a comprehensive literature review of energy-efficient routing protocols for IoT networks, evaluating the performance of these protocols based on key factors such as energy efficiency, latency, packet delivery rates, and security. The current research requires a systematic review, as it allows for the systematic, thorough, and unbiased analysis of existing research on energy-efficient routing protocols.

To achieve the proposed objectives, this study employs the Preferred Reporting Items for Systematic Reviews (PRISMA) methodology, a framework designed to support the reporting and systematic review of literature[14]. The choice of this research design was compared to research designs like Case studies or trials based on the ability to combine and analyze the results of different places, which facilitates the validity and broad applicability of the conclusions. The use of peer-reviewed articles and reliable scholarly resources will provide a strong and valid analysis that will contribute to a profound interpretation and critique of energy-efficient routing protocols applied to IoT networks. Several advantages make a systematic review the most suitable approach in this research. It enables the involvement of different research contributions in different geographical regions of the world, institutional setups, and technological methods of implementation. This method will guarantee full coverage and a better understanding of the subject of energy-efficient routing in IoT networks. Moreover, a systematic review presents the results of research compiled by different reliable sources, which is a more stable base regarding the scale of results and conclusions to make and some recommendations to follow than a case study or case study-like scientific research findings.

3.1 Research Question

This systematic literature review focuses on energy-efficient routing protocols in Internet of Things (IoT) networks. The scope includes identifying frequently used protocols, evaluating their performance based on energy consumption, delay, and security, and analyzing associated trade-offs. The following specific research questions were formulated to guide the study:

- RQ1: Which energy-efficient routing protocols are most frequently applied in IoT networks between 2017 and 2025?
- RQ2: How do various protocols compare in terms of energy usage, delay minimization, and data security?
- RQ3: What trade-offs are evident in the implementation of these protocols across different IoT deployment scenarios?

3.1 Data Source and Search Strategy

The following databases, including IEEE Xplore, Google Scholar, Web of Science, Scopus, and MDPI, were used as part of the comprehensive literature search. These platforms have been chosen to give a wider picture of the up-to-date research in the domain by spanning a wide variety of peer-reviewed journals, conference publications, and technical articles. The search employed the combination of search keywords that constitute routing protocols, energy-efficient. Among significant keywords applied were “Energy-Efficient routing”, “IoT Network”, “Wireless Sensor Networks”, “Routing Protocols”, Network lifetime”, “Latency”, “Packet delivery”. Boolean operators and filters were applied to refine the search results and eliminate irrelevant studies.

3.2 Inclusion and Exclusion Criteria

To ensure the quality and relevance of the selected studies, the following criteria were applied:

Inclusion Criteria:

Studies published between 2017 and 2025

Peer-reviewed journal articles or conference papers

Articles written in English

Research focused on energy-efficient routing protocols for IoT or WSNs

Studies evaluating protocols using performance metrics such as energy consumption, latency, packet delivery ratio, and security

Full-text articles that were openly accessible (open access)[15]

Exclusion Criteria:

Non-English language publications

Studies lacking technical evaluation or performance comparison

Articles unrelated to routing protocols or energy efficiency in IoT

Grey literature, unpublished theses, or blog posts

3.3 The Systematic Literature Review.

Screening and Eligibility

To have a systematic and unbiased search process, all the search results obtained in the chosen academic databases were uploaded to a reference management tool, which helped eliminate duplicates among the sources automatically. After removing duplication, the authors carried out the two-stage screening independently. The initial step was searching and reading the titles and abstracts to remove the unwanted research, including those that have nothing to do with IoT, routing protocols, or energy efficiency of the IoT system. Articles that were unclear as to their relevance at this level were kept to be reviewed in their full text. The second step involved a full text evaluation to ensure that every article fitted the inclusion criteria. We were recording the reasons for exclusion during this stage as well. Papers were excluded if they were: Failure to use energy-efficient routing in an IoT or WSN environment. Didn't do quantitative performance evaluation (e.g., energy consumption, latency, packet delivery). Only dedicated to hardware designs or irrelevant network technologies. Talked about generic networking issues without mentioning modes of energy or routing. Clarity, relevance, and methodological rigor of all selected papers were reviewed. The final source pool was academically sound as the search confined itself to peer-reviewed journals and proceedings of the conference published in the reliable databases. Figure 4 (PRISMA Flow Diagram) shows the study selection process. The database search identified 180 records. The duplicates were eliminated, and 150 new records were left. After screening the titles and abstracts, 100 records were removed. The 50 full-text articles obtained were evaluated for their eligibility, of which 18 were excluded due to non-eligibility. Finally, the synthesis comprised 32 studies.

Included in the search results, the 32 articles selected to form the final pool of this systematic literature review cover 2017–2025 as the latest years of studies, with the years of research in that time frame showing growth in the decade. We found a significant focus in 2024 (25% of the total articles), and the same level of contributions during 2021–2025. This trend indicates that there is an increasing academically perceived interest in undertaking research in energy-efficient routing in an IoT landscape. The annual breakdown of included studies is shown in Table 1.

Table 1
Yearly distribution of articles used for the SLR

Year	Number of Articles	Percentage
2017	2	6.3%
2018	1	3.1%
2019	2	6.3%
2020	3	9.4%
2021	4	12.5%
2022	4	12.5%
2023	4	12.5%
2024	8	25.0%
2025	4	12.5%
Total	**32**	**100**

4. Results

4.1 Categorization of Frequently Used Energy-Efficient Routing Protocols

The systematic literature review revealed various low-energy routing protocols often used in IoT networks between 2017 and 2025. A notable example was RPL (Routing Protocol for Low-Power and Lossy Networks), with its hierarchical, IPv6-based protocol and user-definable objective functions, which would be used in a large number of constrained network contexts. LEACH and L3EACH-V2 (the latter being a variant of the former), are cluster-based protocols characterized by their low-overhead data transfer and energy-efficient clustering algorithm implementation. Since 2023, routing protocols based on AI became widespread, including those based on Grey Wolf Optimization (GWO) and the Salp Swarm Algorithm (SSA), in which the optimal routing paths are optimized in real-time using machine learning. In the meantime, hybrid systems such as HEERPOP and ESEERP provided additional power savings due to multi-path routing and integrated security. The range of protocols, including those based on a chain, SDN, and UAV, indicates the transformative nature of routing strategies that are increasingly adjusted to meet the new requirements and use cases of various IoT applications and deployment settings. These protocols differ in architecture, optimization strategies, and applicability in various IoT uses. Table 2 provides an overview of the most commonly used energy-saving routing protocols found in the literature reviewed. The protocols are organized by the type in which they can be separated, followed by major design features and the time frame in which they were most widely researched. Traceability and

validation sources are given. This tabular presentation aids in tracing major tendencies and new breakthroughs in the sphere of energy-efficient routing in IoT settings

Table 2
Frequently Utilized Energy-Efficient Routing Protocols in IoT Networks (2017–2025)

Protocol	Type	Key Features	Years Highlighted	Reference
Routing Protocol for Low-Power and Lossy Networks (RPL)	Hierarchical	IPv6 support, flexible objective functions (OFs), and reliable LLNs	2019, 2024	[7], [16]
Low-Energy Adaptive Clustering Hierarchy (LEACH)	Cluster-based	Rotating cluster heads, low overhead, baseline WSN protocol	2017, 2023, 2024	[3], [17], [18]
Power-Efficient GAthering Sensor Information System	Chain-based	Sequential transmission, reduced node-to-node distance	2018, 2022	[19]
TEEN/APTEEN	Threshold-based	Reactive protocol, transmits only significant data	2020, 2022	[15]
Lightweight On-demand Ad hoc Distance-Vector Next Generation (LOADng)	Reactive	Lightweight protocol for constrained IoT devices	2019	[7]
ESEERP	Secure Cluster	Multi-path, QoS-aware, energy-efficient, secure	2022	[19]
HEERPOP	Hybrid	Multi-path, QoS-aware, energy-efficient, secure	2024	[18]
RVRR	SDN-based	In-network reducer routing, energy savings, and low RTT	2024	[20]
AI-Based Protocol	Metaheuristic/ Intelligent	Uses ML, fuzzy logic, evolutionary algorithms (e.g., GWO, SSA)	2023–2025	[5], [10]
L3EACH-V2	Cluster-based	Local ID reuse, preamble modulation, underwater IoT, and high energy savings	2023	[21]
PriNergy	RPL-based (QoS-aware)	Content-prioritized routing, TDMA optimization, multimedia support	2020	[22]
UEE-RPL	UAV-assisted Hierarchical	Dual-mode UAV routing, energy-quality metrics	2021	[23]

Protocol	Type	Key Features	Years Highlighted	Reference
		(EEQ, DEQ), delay-efficient		

4.2 Performance Evaluation Based on Energy Consumption, Delay, and Security

These energy-efficient routing protocols provide varying results when compared to essential parameters that include energy consumption, latency, and security. This subsection provides a presentation of how protocols fare in these critical dimensions. Regarding energy consumption, the majority of cluster- and chain-based protocols, including LEACH, L3EACH-V2, and PEGASIS, performed very well, decreasing node-to-node communication distances and enabling sleep scheduling[3], [19], [21]. RPL also exhibited high levels of energy optimization, especially in loss networks. The models of AI-intense routing, such as GWO-based and SSA-based models, significantly and always in normal routing mode, excelled their traditional counterparts in adaptive energy-saving, in particular, in the case of dynamic topologies. Another important performance indicator was latency or delay. Reactive protocols like TEEN and APTEEN were expected to only send out data when critical threshold conditions were encountered, hence low latency in data transmission [15]. Using UAVs to work out hierarchical routing, UEE-RPL showed that data forwarding incurred fewer delays compared to other schemes[23]. RVRR software-defined networking (SDN-based protocol) to further reduce round-trip delays, integrated in-network data reduction [20]. Other protocols, like TEEN and APTEEN, were devised to be reactive, and they sent blocks only when extreme threshold conditions were exceeded, which led to low data latency. UEE-RPL that hierarchically routes them with UAVs exhibited less delay in data forwarding. Software-defined networking (SDN)-based protocol RVRR then incorporates in-network data reduction to reduce round-trip delays further, and applies to real-time IoT applications. Security protection is the most poorly supported component in most protocols. Conventional protocols such as LEACH and TEEN have no inbuilt security measures, and the secure deployment needs extra overheads. However, more recent protocols, like HEERPOP, ESEERP, and PriNergy, included encryption, Qos-aware, and content prioritization techniques and saw enhanced security functionality [22], [24], [25]. Conventional protocols such as LEACH and TEEN have no inbuilt security measures, and the secure deployment needs extra overheads. Yet new protocols, like HEERPOP, ESEERP, and PriNergy, have included encryption, QoS-aware (quality of service), and content-prioritization processes, which have better security characteristics. The use of security, however, may add extra computational expenses, which may compromise energy efficiency in constrained devices.

Table 3
Performance Evaluation Based on Energy Consumption, Delay, and Security

Protocol	Energy Consumption	Delay Performance	Security Support
RPL	High efficiency	Moderate	Low
LEACH	Moderate-high	Low	Low
TEEN/APTEEN	High (Threshold)	Very Low	Low
HEERPOP	High	Moderate	high
ESEERP	High	Moderate	High
AI-Based	Very high (ML-based)	Variable	Moderate
RVRR(SDN)	high	Low RTT	Moderate
UEE-RPL	high	Very Low	Moderate
PriNergy	Moderate	Low	Moderate – high

4.3 Trade-Offs and Implementation Considerations

The protocols discussed have underlying tradeoffs between energy efficiency, delay reduction, and security design [18], [19], [22], [26]. These trade-offs and practical implications of IoT deployment are discussed in this subsection. To explain these trade-offs further, Table 4 provides a synthesis of the literature on the performance of various protocols in the areas of energy efficiency, latency, security, and the generic implementation approach. Each protocol can be viewed comparatively in the table, highlighting the strengths and limitations. As an example, roadmaps such as HEERPOP and ESEERP exhibit high levels of security and energy efficiency, but with the drawback of high implementation complexity, which is well suited to high-stakes applications that consume more computational resources. Conversely, the solutions provided by less-complex protocols like LEACH and TEEN/APTEEN, although being low-complexity protocols with low latency, do not lend themselves well to sensitive applications due to security sacrifice. The AI-supported and UAV-supported protocols demonstrate promising results with high levels of adaptability and performance under changing conditions but might demand more specific infrastructure and increased processing capabilities. This comparison profile will be instrumental in helping researchers and developers to choose unique best-fit routing protocols to the conditions of various IoT applications.

Table 4
Trade-Offs and Implementation Considerations

Protocol	Energy Efficiency	Delay Performance	Security Support	Implementation Complexity
HEERPOP	High	Moderate	High	High
ESEERP	High	Moderate	High	High
AI-Based	Very High	Variable	Moderate	High
LEACH	Moderate-High	Low	Low	Low
TEEN/APTEEN	High (Threshold-based)	Very low	Low	Low
UEE-RPL	High	Very Low	Moderate	Moderate

Also, deployment context plays a significant role in determining a protocol. Specifically, reactive protocols such as TEEN can work well when time is of concern (e.g., industrial monitoring), whereas UAV-supported protocols like UEE-RPL might be more suited to mobile and aerial networks. There is a lack of coherent evaluation metrics of protocols in the literature, which makes it difficult to standardize comparisons; thus, implementing frameworks of benchmarks could be considered in future works.

5. Discussion

5.1. Protocol Design Diversity and Trends

The outcome of this systematic literature review provides results that inform about the challenges and opportunities amid developing and deploying energy-efficient routing protocols within IoT networks. The classification of protocols underscores the variety of methods employed, including clustering and chain-based routing, AI-empowered and SDN-aided [21], [26], [27]. This diversity is representative of the diversity of performance needs and environmental limitations encountered in practical IoT systems. The sheer prevalence of RPL and LEACH in published literature designates their seminal status, but more recent protocols such as HEERPOP, ESEERP, and AI-based models are becoming popular because of their enhanced efficiency and adaptability [16], [18], [19].

5.2. Performance Analysis: Energy, Delay, and Security

Energy usage is a predominant issue, sometimes taking preference over latency or security. Energy-efficient protocols such as LEACH and PEGASIS rely on data aggregation and node rotation and are therefore restricted in terms of providing secure and low-latency communication [3], [21]. Hybrid protocols (e.g., HEERPOP and ESEERP), on the other hand, and models with AI offer a more even solution, where QoS and basic security options are accompanied by energy savings. Their complexity and computational requirements also might not be compatible with low power settings [25], [26].

Latency-based protocols like TEEN and UEE-RPL have the advantage of real-time data processing, but might drop updates that do not present specific consequences or have the overhead of extra infrastructure such as UAVs [15], [23]. Despite AI-based solutions fitting the dynamics of networks relatively well, they are quite resource-intensive and can cause learning-induced delay. The fact that no universal protocols score universally high shows that performance is highly contextual.

5.3. Performance Analysis: Energy, Delay, and Security

Security is a significant issue in the design of routing protocols. Not many protocols have built-in encryption or prioritization strategies. The majority relies on an external layer to provide data security, which further complicates the overall design of systems and can impact energy performance [19], [19], [22]. This presents a possibility of cross-layer protocol designs focusing on combining energy efficiency and lightweight, in-protocol security features.

5.4. Contextual Suitability and Future Direction

The review signifies the importance of end-to-end, application-conscious protocol design. Depending on deployment requirements in terms of topology, node capacity, mobility, and sensitivity of the data being transmitted, protocol designers need to balance trade-offs in terms of energy consumed, latency, and security. The work in the future should be concentrated under adaptive and scalable solutions, where an optimization of cross-layer as well as the real-world validation should be encompassed to provide further robustness and practicality in routing protocols in various IoT applications.

6. Conclusion

The present systematic literature review presents analyses of 32 peer-reviewed articles published in 2017–2025, covering the topic of energy-efficient routing protocols within IoT networks. Three decisive research questions guided the study: what are the widely adopted protocols, how well do they fare regarding energy consumption, latency, and security, and what are their trade-off characteristics? It was established in the review that the widely used protocols like RPL, LEACH, TEEN, and hybrid schemes like HEERPOP and ESEERP have been used because of their energy-conservation features and structural optimization potentials. But no scheme performed well in all measurements. Although some protocols emphasize their low energy consumption, they tend to lack delay mitigation or security measures. On the other hand, those with more secure protocols would consume more computation resources, and therefore, they would be less compatible with limited devices. The results indicate that protocol choice in IoT is context-specific. Design decisions must reflect the needs of a given application, real-time communication, sensitive data, or device constraints. Moreover, not many protocols have extensively incorporated native security tools, which leads to the urgent necessity of lightweight, extensible, and dynamic solutions.

6.1. Limitations of the Study

Although the research was conducted as per PRISMA 2020 to guarantee methodological rigor, it is worth mentioning a few limitations. First, being restricted to English publications and published (grey) literature might have reduced the range of reflective perspectives included in this review. Second, the search itself was limited by date and type to peer-reviewed articles within 2017–2025, which could either miss the earlier formative texts or the latest breakthroughs after the search date. The study also omitted those protocols that had not been explicitly focused on energy-efficient protocols, potentially at the expense of routing models that might be successful in practice but not formulated in the context of energy-saving requirements.

6.2. Future Research

In future work, more emphasis should be placed on creating holistic routing schemes that establish a balance between energy, performance, and security, and are scalable and feasible to implement. Benchmarking models and practical validation will also be critical to the development of energy-efficient routing protocol design and selection within next-generation IoT networks.

Declarations

Funding

No funding was received to support this study

Author Contribution

1. Substantial contributions to concept or designAcquisition, analysis, or interpretation of dataDrafting of the manuscriptCritical review of the manuscript for important intellectual contentAgreed to be accountable for all aspects of the workWill review the final version to be published2. Substantial contributions to concept or designAcquisition, analysis, or interpretation of dataCritical review of the manuscript for important intellectual contentAgreed to be accountable for all aspects of the workWill review the final version to be published3. Substantial contributions to concept or designCritical review of the manuscript for important intellectual contentAgreed to be accountable for all aspects of the workWill review the final version to be publishedSupervised the work4. Substantial contributions to concept or designCritical review of the manuscript for important intellectual contentAgreed to be accountable for all aspects of the workWill review the final version to be publishedSupervised the work

References

1. Zhang, J. A., et al. (2021). Enabling joint communication and radar sensing in mobile networks—A survey. *Ieee Communication Surveys And Tutorials*, *24*(1), 306–345.
2. Mouha, R. A. R. A. (2021). Internet of things (IoT). *J Data Anal Inf Process*, *9*(02), 77.

3. Kaur, G., Chanak, P., & Bhattacharya, M. (2021). Energy-efficient intelligent routing scheme for IoT-enabled WSNs. *IEEE Internet Things J*, *8*(14), 11440–11449.
4. Yadav, R. and V. and, & Kumar, A. (May 2024). Systematic Review Paper on Energy-Efficient Routing Protocols in Internet of Things. *IETE J Res*, *70*(5), 4721–4743. 10.1080/03772063.2023.2230169
5. Suryawanshi, V. (Sep. 2024). Advancements in IoT Routing and Energy Efficiency: A Comprehensive Review of Algorithms and Technologies. *Sci Manag Des J*, *2*(3). 10.70295/SMDJ.2409024
6. Bekal, P., Kumar, P., Mane, P. R., & Prabhu, G. (2024). A comprehensive review of energy efficient routing protocols for query driven wireless sensor networks [version 3; peer review: 2 approved].
7. Magubane, Z., Tarwireyi, P., & Adigun, M. O., Evaluating the Energy Efficiency of IoT Routing Protocols, in 2019 *International Multidisciplinary Information Technology and Engineering* Conference *(IMITEC)*, Nov. 2019, pp. 1–7. 10.1109/IMITEC45504.2019.9015904
8. Dubey, A., & Yadav, S. K. (Oct. 2024). Basics of Internet of Things. *INTERNATIONAL J Sci Res Eng Manag*, *08*(10), 1–6. 10.55041/IJSREM37970
9. Ud Din, I., et al. (2019). The Internet of Things: A Review of Enabled Technologies and Future Challenges. *Ieee Access : Practical Innovations, Open Solutions*, *7*, 7606–7640. 10.1109/ACCESS.2018.2886601
10. A. T. S, Energy-Efficient IoT Networks: Optimizing Resource Management through Machine Learning, *Commun. Appl. Nonlinear Anal.*, vol. 32, no. 1s, Art. no. 1s, (2025). 10.52783/cana.v32.2168
11. Kaur, N., & Sood, S. K. (Jun. 2017). An Energy-Efficient Architecture for the Internet of Things (IoT). *Ieee Systems Journal*, *11*(2), 796–805. 10.1109/JSYST.2015.2469676
12. Mwewa, W., & Lubobya, S. C. (Mar. 2022). Performance Evaluation of Routing Protocols in Enterprise Networks. *Am J Comput Eng*, *5*(1), 24–35. 10.47672/ajce
13. Rani, P., & Sangwan, A. A Review on Routing Protocols in Wireless Sensor Networks. *Eng Technol*.
14. Page, M. J., et al. (Mar. 2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *PLOS Med*, *18*(3), e1003583. 10.1371/journal.pmed.1003583
15. Goswami, P., et al. (Feb. 2022). AI-Based Energy Efficient Routing Protocol for Intelligent Transportation System. *Ieee Transactions On Intelligent Transportation Systems*, *23*(2), 1670–1679. 10.1109/TITS.2021.3107527
16. Yadav, R., & Kumar, V. (May 2024). A Systematic Review Paper on Energy-Efficient Routing Protocols in Internet of Things. *IETE J Res*, *70*(5), 4721–4743. 10.1080/03772063.2023.2230169
17. Dass, R., et al. (Jul. 2023). A Cluster-Based Energy-Efficient Secure Optimal Path-Routing Protocol for Wireless Body-Area Sensor Networks. *Sensors (Basel, Switzerland)*, *23*(14), 6274. 10.3390/s23146274
18. Shial, R. K., Rath, P., Patnaik, S. R., & Ghuar, U. (2024). HEERPOP: Hybrid Energy Efficiency Routing Protocol for Optimal Path in the Internet of Things-Based Sensor Networks, *Int. J. Comput. Netw. Appl.*, vol. 11, no. 4, pp. 494–505, Aug. 10.22247/ijcna/2024/31

19. Dogra, R., Rani, S., Kavita, J., Shafi, S., Kim, & Ijaz, M. F. (Aug. 2022). Enhanced Smart Energy Efficient Routing Protocol for Internet of Things in Wireless Sensor Nodes. *Sensors (Basel, Switzerland)*, *22*(16), 6109. 10.3390/s22166109
20. Hadi, T. H. (Apr. 2024). IoT Protocols: Connecting Devices in Smart Environments. *ICST Trans Scalable Inf Syst*. 10.4108/eetsis.5665
21. Ghazy, A. S., Kaddoum, G., & Singh, S. (2023). Low-Latency Low-Energy Adaptive Clustering Hierarchy Protocols for Underwater Acoustic Networks. *Ieee Access : Practical Innovations, Open Solutions*, *11*, 50578–50594. 10.1109/access.2023.3277395
22. Safara, F., Souri, A., Baker, T., Al Ridhawi, I., & Aloqaily, M. (2020). PriNergy: a priority-based energy-efficient routing method for IoT systems, *J. Supercomput.*, vol. 76, no. 11, pp. 8609–8626, Nov. 10.1007/s11227-020-03147-8
23. Yang, Z., Liu, H., Chen, Y., Zhu, X., Ning, Y., & Zhu, W. (2021). UEE-RPL: A UAV-Based Energy Efficient Routing for Internet of Things, *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1333–1344, Sep. 10.1109/TGCN.2021.3085897
24. Dogra, R., Rani, S., & Gianini, G. (2023). REERP: A Region-Based Energy-Efficient Routing Protocol for IoT Wireless Sensor Networks, *Energies*, vol. 16, no. 17, p. 6248, Aug. 10.3390/en16176248
25. Shial, R. K., Rath, P., Patnaik, S. R., & Ghuar, U. (2024). HEERPOP: Hybrid Energy Efficiency Routing Protocol for Optimal Path in the Internet of Things-Based Sensor Networks, *Int. J. Comput. Netw. Appl.*, vol. 11, no. 4, pp. 494–505, Aug. 10.22247/ijcna/2024/31
26. Suryawanshi, V. (Sep. 2024). Advancements in IoT Routing and Energy Efficiency: A Comprehensive Review of Algorithms and Technologies. *Sci Manag Des J*, *2*(3). 10.70295/SMDJ.2409024
27. Magubane, Z., Tarwireyi, P., & Adigun, M. O., Evaluating the energy efficiency of IoT routing protocols, in 2019 *International Multidisciplinary Information Technology and Engineering* Conference *(IMITEC)*, IEEE, 2019, pp. 1–7. Accessed: May 21, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9015904/?casa_token=cQSQ3suJzJ8AAAAA:p4sjyvMSD926_v3_4FHMewekyHjRebXaZ4jq77sJVI-8SkAAnZRrsaT484E7tJpywQadRxwi8WORVdiz

Figures

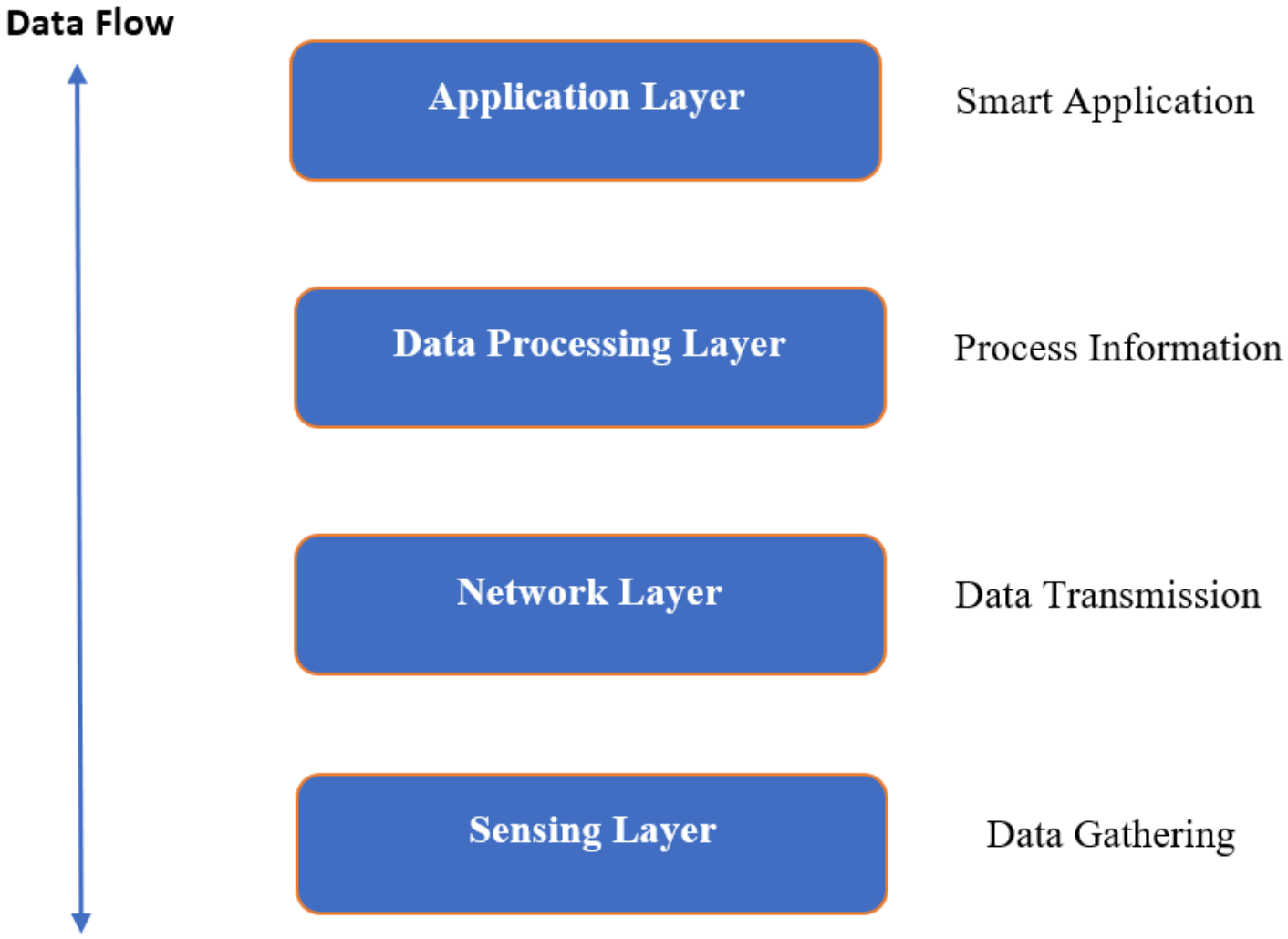

Figure 1

Internet of Things (IoT) architecture

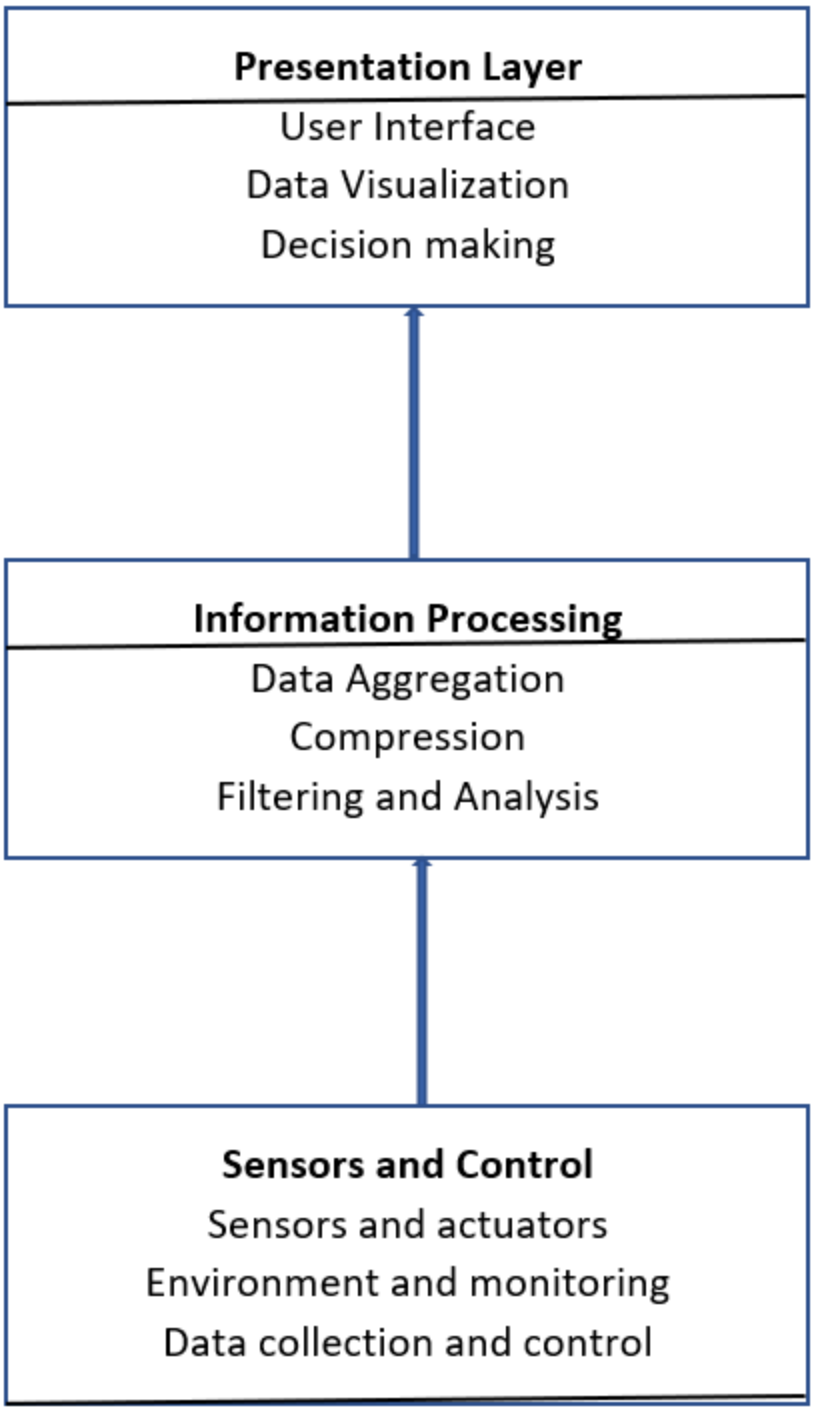

Figure 2

Energy-efficient Architecture for IoT Networks

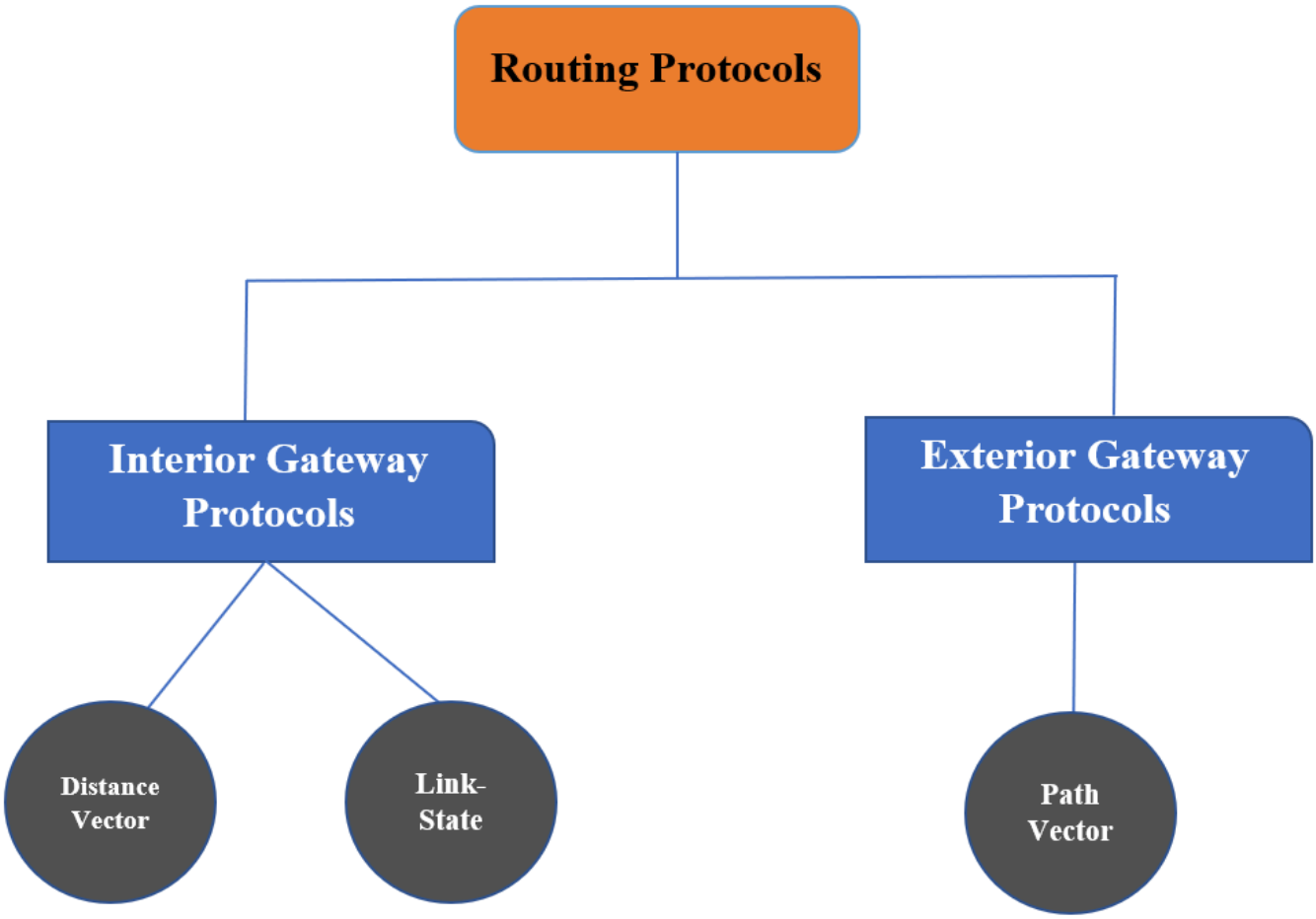

Figure 3

Types of Routing Protocols

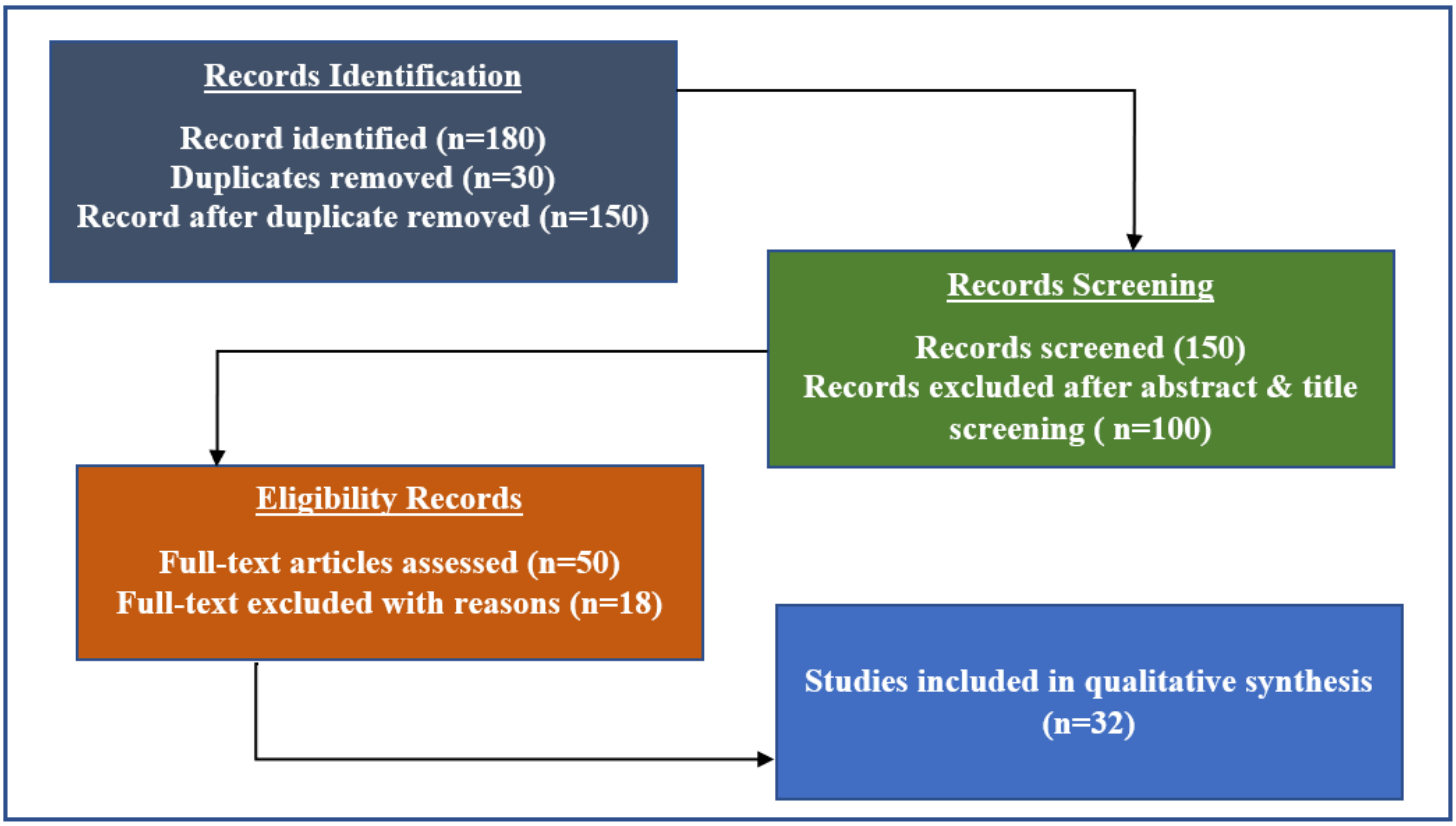

Figure 4

shows the PRISMA framework for this study