A Review of Energy Efficient and Secure Routing for Internet of Things Based Wireless Sensor Networks

Rajesh M R[1], Abdul Rasheed[1], Thangavel K[1], Prema R[1]

[1]*Department of Electronics and Communication, Hindusthan College of Arts and Science, Coimbatore, India.*

Corresponding mail: rajeshmrsn@gmail.com

***Abstract*: The integration of Wireless Sensor Networks (WSNs) with the Internet of Things (IoT) has revolutionized a wide range of industries, from environmental monitoring to industrial automation. The two major challenges of WSN are energy efficiency and network security. Designing a routing protocol considering both energy efficiency and security is a critical challenge due to the constrained nature of nodes and their susceptibility to malicious attacks. Additionally, the routing protocols designed for conventional WSNs are not suitable for IoT-based WSNs because of their diverse and complex nature. This survey presents a review of energy-efficient and secure routing models specifically designed for IoT-based WSN from the years 2019 to 2025. The collected routing models are categorized as energy-efficient, energy and security based, and energy and trust-based schemes. An analytical summary of routing protocols focusing on factors such as energy efficiency, heterogeneity, scalability, data aggregation, multipath, quality of service and multi-hop communication is presented. Finally, the survey addresses open issues, challenges, and future directions within the field, thereby motivating forthcoming research works.**

***Keywords*: Energy-efficiency, security, routing, WSN, and Internet of Things.**

1. Introduction

The Internet of Things (IoT) is a network in which physical devices, equipment, sensors, and other things communicate with each other without human involvement. The purpose of the IoT is to provide seamless connectivity and services to anything, anywhere, at any time [1], [2]. Human life is significantly impacted in many aspects by IoT in terms of convenience, enhanced experiences, and efficiency [3]. The number of devices connected to the Internet, those with digital identity, is increasing day by day, and as indicated by Cisco, there will be 500 billion devices connected with the IoT by 2030 [4].

Wireless Sensor Network (WSN) is an integral part of the IoT network because it acts as one of the sources of data for the elements of the Internet of Things [5], [6]. It makes the bridge between the digital world and the real world. A WSN is a collection of tiny sensing devices or nodes that perform communication with other devices through a wireless channel. Technological developments in sensors make it possible to build low-cost and tiny-sized IoT-enabled wireless sensors to bring smartness to small-to large-scale appliances.

A typical WSN is composed of numerous numbers of sensor nodes with sensing, communication, and processing capabilities [7]. The challenges in the design of WSNs are energy conservation, scalability, localization, security, routing, etc [8]. WSN can dynamically alter the network structure due to various external events, such as node mobility, environmental changes, and the addition or removal of nodes, to optimize the effectiveness of the network [3]. An IoT-based WSN is made up of various specialized sensors used for various applications like animal monitoring, environmental sensing, disaster management, habitat monitoring, intelligent transportation, healthcare, transport, armed forces surveillance, and weapon control [7], [9].

Two of the major challenges in WSN are energy management and security [2], [10]. The major role of a sensor is to sense the environment, gather and transmit the data to the base station. But the battery equipped sensor nodes hold only limited and non replaceable energy resources. Therefore, the energy-constrained sensor nodes must be utilized effectively to extend the network lifetime. Various approaches have been proposed to enhance the network's lifetime. Energy conservation during data transmission from source to destination is a main focus in WSN. Clustering and cluster-based routing protocols are used in WSN to improve the energy consumption and network lifetime [1],[7],[10]. The cluster-based routing protocol, where the sensor nodes are divided into small clusters, is an effective technique to reduce energy consumption by avoiding long-distance communication. Each cluster employed one node as a cluster head (CH), each member node sends its sensed data to its cluster head, and which thereafter sends it to the base station either a single-hop or multi-hop manner. To provide data security in WSN is a difficult task because it is a highly resource-constrained network. The network should ensure data confidentiality, data integrity, data reliability, secure data transmission, and access control [12]. Routing protocols of WSNs are affected by various attacks such as Sybil attacks, selective forwarding attacks, wormhole attacks, black hole attacks, sinkhole attacks, and hello flooding attacks [7]. WSNs need reliable, effective, and resilient routing protocols to counter the aforementioned attacks.

The major contribution of this review is as follows:

1. This paper offers an insight into different existing approaches and algorithms and optimization techniques that are used to overcome the issues regarding the efficient routing in IoT-based WSN.
2. The taxonomy of various routing schemes, such as energy-efficient routing, energy and security-based routing, and energy and trust-based routing models in IoT-based WSN, is exhibited.
3. This paper presents and compares the methodology, advantages, performance evaluation metrics, and future directions of the protocols.
4. A summary of routing protocols focusing on factors such as energy efficiency, heterogeneity, scalability, data aggregation, multipath, Quality of Service (QoS), multi-hop communication, and simulation techniques is presented.
5. This paper highlights some of the open issues and challenges in this research domain.

The rest of the paper is organized as follows: Section 2 discusses the literature works collected for review. Section 3 conducts a summary and analytical discussion on state-of-the-art routing protocols. Section 4 discusses the open issues and challenges in designing efficient and secure routing protocols. Section 5 concludes the paper along with future directions.

2. Literature Review

A. Energy Efficient Routing

Dwivedi et al. [13] proposed a two-stage routing protocol (EETSP) to diminish the communication overhead and enhance the lifespan of WSN. EETSP consisted of two stages; the cluster head and secondary cluster head were selected in the first stage, and intercluster routing and intracluster routing were performed in the second stage. The parameters considered for the selection of the cluster head were the distance to the base station (BS), centrality, neighbours' density, and residual energy. The simulation results indicated that the EETSP provided better performance in terms of stability period, throughput, and overall network lifetime in comparison to existing methods.

S. Tumula et al. [14] introduced an opportunistic energy-efficient dynamic self-configuration routing (OEDSR) algorithm to alleviate problems due to congestion in IoT-based WSN. In this method, the optimal route to the base station is calculated by using the residual energy and mobility factor of the sensor nodes obtained through a routing tree model based on graph theory. The OEDSR considered a hybrid network with multiple gateways to mitigate problems due to node failure. The Steiner tree algorithm has been used for cluster formation. The suggested methodology reduced energy consumption and end-to-end delay when compared with current methods.

A new zone-based and event-driven protocol (TESEES) was developed by Abdul-Qawy et al. [15] to reduce energy consumption in sensing nodes by avoiding unnecessary frequent data transmission. This protocol addressed the limitations of the traditional SEES protocol and is a reactive version of the proactive SEES protocol. TESEES supported multilevel heterogeneity and was suitable for large-scale IoT-based WSN. The authors also employed a hybrid TMCCT algorithm by which, for each reporting interval, only the zone member nodes whose sensed data meet the given requirements were allowed to send their data to the base station through relay nodes. The protocol effectively reduced unnecessary data transmissions, leading to improved energy efficiency.

Gupta et al. [16] proposed an energy efficient data communication (EEDC) scheme. This scheme utilized a multi-tier hierarchical clustering framework to provide network load balancing in scalable WSN-IoT environments. The EEDC considered a rectangular network area where all the nodes in it were stationery and uniform. The network was divided into various regions, and each region had sub-regions. The area covered by regions kept on decreasing towards BS, and the number of sub-regions in each region kept on increasing towards BS to ensure even load distribution across all network nodes. The suggested methodology reduced energy usage in sensor nodes and improved the packet drop ratio.

To enhance energy efficiency and prolong the network lifespan, Nguyen & Tan et al. [17] introduced the hybrid routing protocol (HRP-EE) in WSN for IoT applications. It was a cluster-based protocol in which the cluster head is selected based on the residual energy level of nodes, the node's distance to others within the cluster, and node density. The Voronoi diagram-based clustering routing mechanism was employed to reduce intra-cluster data communication costs. The HRP-EE was a hybrid method that integrated both the minimum spanning tree and Dijkstra's algorithm for determining the optimal path. Simulation results revealed that HRP-EE outperformed existing protocols such as LEACH-VA, PEGCP, and TBC in terms of energy efficiency and network lifespan.

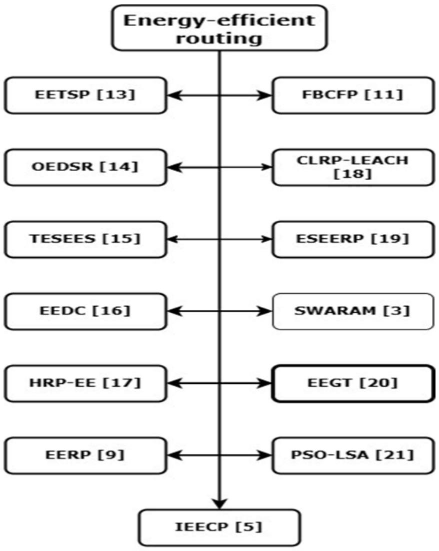

Fig. 1. Taxonomy of energy-efficient routing

Table 1
Relevant literature on energy-efficient routing

Protocol & Reference.	Performance evaluation metrics	Advantages	Future scope
EETSP [13]	Average energy, stability period, alive node, dead node and throughput.	Better performance in terms of average energy, stability period, and throughput.	Enhancement to work with mobile sensor nodes in IoT agriculture.
OEDSR [14]	Packet delivery ratio (PDR), throughput, end to end delay, energy consumption and network lifetime.	Decreased energy consumption, increased throughput and provided reliability.	To provide optimized data management for WSNs.
TESEES [15]	Total energy saving, the lifetime extension and average energy consumption.	Enhanced energy savings, network lifetime and reduced traffic load.	To enhance protocol by comprehensively addressing various aspects of network settings.
EEDC [16]	Throughput, energy consumption and number of alive nodes.	Reduced energy usage and improved packet drop ratio.	Enhance by applying block chain-based security solutions.
HRP-EE [17]	Network lifespan, energy efficiency and throughput.	Improved network lifespan, energy efficiency and throughput.	Aim to refine energy-efficient routing protocol for IoT -centric WSNs.
EERP [9]	Number of rounds. first node dies, last node dies and energy consumption.	Reduced energy consumption and minimized the transmission of redundant data.	To enhance performance by using soft computing techniques.
IEECP [5]	Network life time, energy dissipation and number of messages arrived at the base station.	Reduced and balanced the energy consumption of nodes.	Enhance the protocol by improving the FCM algorithm.
FBCFP [11]	Energy utilization, packet delivery ratio, delay and network lifetime.	Better performance in terms of energy utilization and system life span.	Enhance the protocol by using a new trust mechanism.
CLRP- LEACH [18]	Average energy consumption, network lifetime and average end-to-end delay.	Increased network life time.	Develop a secure lightweight encryption scheme for cloud-based services.
ESEERP [19]	Energy efficiency, bandwidth, packet delivery ratio and network longevity	Increased packet delivery ratio and better performance in network life time.	Improve the efficiency by using cluster optimization.
SWARAM[3]	Network lifespan, average energy consumption, Packet delivery to sink.	Improved the packet delivery ratio and network lifetime.	To analyze the protocol performance in a real-time environment.
EEGT [20]	Network life time and energy efficiency.	Better performance in energy efficiency and the network lifespan.	Design efficient protocols for under water smart micro-sensor for unauthorized intrusion detection.
PSO-LSA & SA-LSA [21]	Number of clusters created, average end-to-end delay, average packet loss rate and lifetime computation.	Reduced isolated nodes, improved connectivity and enhanced lifespan.	Enhance SA-LSA algorithm to address multi-objective problems more effectively.

Pedditi & Debasis [9] developed an energy-efficient routing protocol (EERP). This is a time division multiple access-based medium access control protocol to extend the lifetime of IoT-based WSN systems used for forest fire detection. The model decreased the energy utilization in sensor nodes by minimizing idle listening in cluster heads. In this method only the sensor nodes close to an event were allowed to report it; this minimized the transmission of redundant data. The simulation results proved that the proposed model performed better in reducing the energy consumption in sensor nodes and extending the lifetime of WSNs.

Hassan et al. [5] developed an improved energy-efficient clustering protocol (IEECP) to prolong the lifetime of the WSN-based IoT. The main objective of this method was to address the issues related to the poor clustering structure in WSN. The proposed IEECP consisted of three parts. Firstly, an optimal number of clusters were determined based on a mathematical model. Secondly, a modified fuzzy C-means algorithm was proposed to create balanced clusters. Thirdly, a new algorithm called the CH selection and rotation algorithm was introduced that integrated the back-off timer mechanism for the selection and rotation of CH for clusters.

Thangaramya et al. [11] proposed a neuro-fuzzy rule based clustering approach (FBCFP) to enhance the performance of IoT-based sensor networks. This work suggested a deep learning-based approach integrated with a Neuro-Fuzzy Inference System for the extension of network lifetime. The authors of this intelligent routing considered four parameters for cluster formation, namely, residual energy of the cluster head, the space between the cluster head and the sink node, the space between the sensor node and the cluster head and the degree of the cluster head. The simulation results of the proposed method showed improved performance in terms of energy utilization and system lifespan.

Nasri et al. [18] created two protocols: one is a fuzzy-based routing protocol (FRP-LEACH) and the second is a cross-layer routing protocol (CLRP-LEACH) for an IoT-enabled WSN environment to enhance the network lifetime. The proposed algorithms were based on clustering topology and designed for IoT healthcare applications. In the FRP-LEACH protocol, the sensor nodes executed a fuzzy module to determine their cluster heads for the next cycle. This is a distributed algorithm. CLRP-LEACH used a cross-layer design that enhanced communication efficiency by allowing interaction between the network layer, MAC layer, and physical layer. The simulation result showed that the proposed methods prolong the network lifetime.

To solve the issue of sensor nodes near the base station having a short lifespan, Dogra et al. [19] presented sailfish optimization based routing protocol (ESEERP) for IoT in

WSNs. The three primary stages in the proposed scheme are data aggregation, multi-objective-based selection of cluster heads and optimization-based path selection for data transfer. The SFO is a bio-inspired algorithm that used the hunting behavior of sailfish to find optimal paths for the transmission of data. The simulation results showed improved performance in terms of energy utilization, network longevity, bandwidth of transmitted data and packet delivery ratio in comparison to the existing protocols.

Somula et al. [3] developed an optimized energy-efficient cluster head selection protocol (SWARAM) to address the problem of the energy-hole issue in WSN-based IoT. This method used Euclidean distance to form clusters with a group of nodes and the Osprey Optimization Algorithm (OOA) for CH selection. Compared to other optimization algorithms, the coverage time during the CH rotation process is quick in OOA. The simulation result showed that the SWARAM protocol improved the packet delivery ratio and network lifetime when compared to the existing methods.

Duy Tan et al. [20] introduced an energy-efficient routing protocol based on grid cells (EEGT) to minimize energy consumption with in data transmission paths in homogeneous and heterogeneous network models in WSN-based IoT applications. In this method, a cluster head node is chosen according to the residual energy and the distance between the sink and nodes in each cell. EEGT constructed multi-hop data transmission paths for intra-cells and inter-cells based on the minimum spanning tree and ant colony algorithm (ACO). The simulation results indicated that the performance of the proposed protocol was better than the existing methods in terms of energy efficiency and the lifespan of the network.

Senthil et al. [21] created an O-LEACH protocol, which specifically addressed the issue of orphan nodes in WSN. The nodes that were not part of any cluster were known as orphan nodes. The protocol ensured that these nodes were included in the clustering process, which helped improve network connectivity and reliability. The authors also proposed hybrid optimization techniques using simulated annealing with the lightning search algorithm (SA-LSA) and particle swarm optimization with LSA (PSO-LSA) algorithms for IoT-based WSN for the minimization of the isolated nodes. These proposed techniques effectively managed the cluster head selection, achieved optimal path routing, and minimized energy usage.

The taxonomy of energy-efficient routing models is shown in Figure 1. A comparative analysis of energy-efficient routing protocols based on performance metrics, advantages, and future scope is described in Table 1.

B. Energy and Security Based Routing

Jain et al. [22] introduced an energy-efficient and secure route adjustment (ESRA) with security support in an IoT-WSN environment. The proposed system used two levels of security: biometric based authentication and data encryption by Rivest-Shamir-Adleman (RSA) and Secure Hash algorithm 1(SHA-1) methods. The sensor nodes are given a time interval for data transfer; for that, a new threshold-based timeslot scheduler was employed in this method. A type-2 mamdani fuzzy logic system is established to determine the shortest path list. The authors claimed the proposed method provided the security of data transmission along with reduced energy consumption and packet loss rate in IoT-WSN compared to previous methods.

Haseeb et al. [23] presented an energy-efficient and secure (EES) IoT-based WSN framework for smart agriculture applications. The primary objective of the proposed framework is to select the more suitable cluster heads based on a multi-criteria decision function. The decision is based on residual energy, distance to base station, and signal-to-noise ratio factors. Moreover, the proposed framework used the recurrence of the linear congruential generator for secure data transmission from sensor nodes towards the base station based on secret keys. Single-hop communication was employed in this method.

To address the major two challenges of WSNs, namely security and energy, Hussein et al. [10] proposed an elliptic curve cryptography (ECC) based scheme. The proposed E-LEACH protocol used a combination of a distributed key exchange and management methods based on ECC to ensure the security of node communication. An improved version of the LEACH routing protocol was employed to maximize the lifetime of the network. The authors claimed that the protocol demonstrated better performance in parameters such as network lifespan and energy consumption.

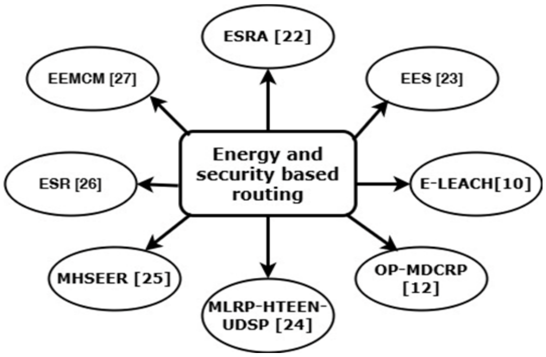

Fig. 2. Taxonomy of energy and security-based routing

Loretta G. & Kavitha [12] suggested an optimal privacy multi-hop dynamic clustering routing protocol (OP-MDCRP) to avoid the data-privacy based cryptography attacks in the WSN-based IoT. OP-MDCRP employed an integrated encryption scheme that uses ECC based public-key encryption and a symmetric cipher for high data privacy and integrity. This method used both clustering and multi-hop communication to reduce the energy consumption of sensor nodes. Simulation results indicated that the OP-MDCRP approach provided more data security than existing methods in terms of computational time, PDR, energy consumption, average delay, network overhead, and network lifetime.

Nagaraju et al. [24] presented an energy-optimized secure routing scheme for IoT applications in heterogeneous WSNs. In this scheme, secure routing was established for confidential data of the IoT through sensor nodes using the multipath link routing protocol; the energy and network lifetime were improved using the hybrid-based TEEN protocol, and the data storage capacity was improved using the ubiquitous data storage protocol. This technique employed a light-weight distributed key management scheme for secure communication. This routing protocol has been implemented and compared with existing routing protocols, and it showed an improvement in performance parameters such as throughput, energy efficiency, end-to-end delay, network lifetime, and data storage capacity.

Table 2
Relevant literature on energy and security based routing schemes

Protocol & Reference	Performance evaluation metrics	Advantages	Future scope
ESRA [22]	Connectivity ratio, energy consumption, delay, Packet loss rate and encryption time.	Higher connectivity ratio, and improved packet loss rate	Implement the proposed method in real-world application.
EES [23]	Throughput, packets drop ratio, network latency, energy consumption and routing over head.	Decreased energy consumption, improved data delivery and secured data transmission.	Enhancement to handle mobility.
E-LEACH [10]	Number of rounds, energy consumption, time consumption, dead nodes and hop counts	Enhanced security in WSNs. Improved energy efficiency and network lifespan	Evaluate the method's robustness to various types of attacks for a 3D network application.
OP-MDCRP [12]	Computational time, PDR, energy consumption, average delay, network overhead and network lifetime.	Better data privacy, less energy consumption, high data delivery ratio, less delay and low network overhead.	Implement the protocol using real-world datasets.
MLRP-HTEEN-UDSP [24]	Throughput, end-to-end delay, network life time, data storage and energy efficiency.	Higher throughput, minimum end to end delay. Better network life time and data storage capacity.	Evaluate the protocol performance in large green IoT network.
MHSEER [25]	Throughput, packet drop ratio, end to end delays, energy consumption and faulty rout analysis.	Increased throughput, Decreased PDR, packet delay, energy consumption, and faulty pathways.	Implement the protocol using real-world datasets.
ESR [26]	Network lifetime, average end to end delay, PDR, average communication cost and network overhead.	Improvement in network lifetime, end- to-end delay, PDR, average communication cost and network overhead.	Enhancement to handle mobility along with multi-hop network.
EEMCM [27]	Energy consumption, network life time, PDR, packet loss ratio, scalability and end to end delay.	Excellent anomaly detection and energy efficiency.	To test protocol performance in a real time environment.

Sharma et al. [25] developed a meta-heuristic secure and energy-efficient routing (MHSEER) protocol for wireless sensor-based industrial IoT. The objective of this study is to propose a WSN routing technique that is secure and energy-efficient. The protocol consisted of two stages. The first stage used a heuristics method to estimate the relative weight for locating the best node on the next hop. In the second stage, a computationally simple and random counter encryption mode was used for security. The proposed protocol, when compared with existing methods, increased throughput and decreased the packet drop ratio, packet delay, energy consumption, and faulty pathways.

Haseeb et al. [26] designed an energy-efficient and secure routing protocol (ESR) for intrusion avoidance in an IoT-based WSN. The objectives of this scheme are to increase the network period and data trustworthiness. This method introduced a clustering mechanism that has optimized the selection of cluster heads based on the intrinsic qualities of nodes. The protocol employed a threshold-based Shamir secret sharing scheme, which ensured the reliability and security of data transmission.

Thangavel & Rajendran [27] introduced an innovative energy efficient clustering method (EEMCM) to address energy consumption and security challenges in heterogeneous-IoT WSNs. The proposed method utilized the parallelized memetic algorithm for cluster formation and cluster head selection. The model employed a chi-squared test for feature selection and AlexNet architecture for anomaly detection to improve the network performance and reduce energy consumption. The paper claimed that the proposed method achieved an accuracy of 99.11% in anomaly detection in IoT WSNs.

The taxonomy of energy and security based routing models is shown in Figure 2. A comparative analysis of energy and secure based routing protocols is described in Table.2.

C. *Energy and Trust Based Routing*

A three-tier clustering routing protocol was developed by Ilyas et al. [7] with an embedded check-up node to encounter malicious activities of nodes and to slant them to the backlist. The protocol employed the K-means and fuzzy-C-means algorithms for the cluster formation. The hardware-based link quality estimators are considered in this work to further improve the routing efficiency. The simulation result showed that the proposed protocol outperformed the existing methods in terms of network lifetime, network throughput, average energy consumption, network stability, and packet latency.

Rajeswari et al. [2] proposed the trusted energy efficient fuzzy logic based clustering algorithm (TEEFCA), which addresses the security and energy efficiency design challenges in WSN-based IoT. In this method, the trustworthy nodes are identified, which may act as candidate nodes for cluster-based routing. Then the fuzzy inference system was employed under the two circumstances, namely the selection of an optimal cluster leader and the cluster formation process. The TEEFCA showed significant improvement in terms of power conservation, network stability and lifetime when compared to the existing cluster-aware routing approaches.

Mishra et al. [28] developed a trust-based PSOGA model to increase the network lifetime in an IoT-based WSN environment. The proposed model employed a two-step approach. The first step employed a trust model to select the cluster heads that manage the data communication between the BS and nodes in the cluster. Further, a novel hybrid algorithm, which is comprised of a particle swarm optimization (PSO) algorithm and a genetic algorithm (GA), is proposed to determine the routes for data transmission.

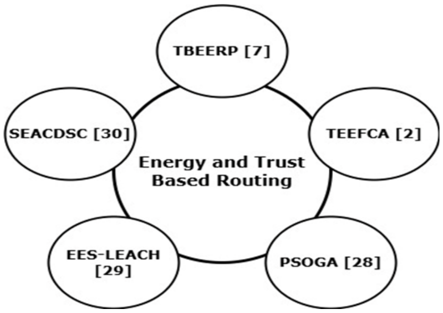

Fig. 3. Taxonomy of energy and trust based routing

Suresh & Shayma [29] introduced an EES-LEACH protocol, which is an enhanced version of the LEACH procedure to stabilize the cluster head selection in WSN for IoT networks. In this scheme the random number generation is made dependent on the node quality of the network's nodes. In EES-LEACH, the cluster heads are selected based on the following parameters: node coverage, energy consumption rate, and distance to the base station. A trust-based secure relay selection technique has been introduced into the routing path to eliminate malicious nodes, which further improved the relay node selection and secure data transfer.

Osamy et al. [30] created a novel clustering technique that chose secure CHs utilizing trust parameters for IoT-enabled WSN-based applications. The authors formulated an effective fitness function, which considered the sensor node's trust value and the remaining energy for the reliable selection of CHs. The proposed method introduced a discrete sand cat swarm optimization (SCSO) method, a variant of the traditional SCSO, designed to tackle optimization problems where the solution space is discrete. The stimulation result proved that the proposed method performed well when compared with existing methods in terms of stability, reliability, and network lifetime.

The taxonomy of energy and trust based routing models is shown in Figure 3. A comparative analysis of energy and trust based routing protocols is described in Table 3.

3. Summary and Analytical Discussion on State of Art Routing Protocols

The summary of routing protocols focusing on energy efficiency, heterogeneity, scalability, data aggregation, multipath, QoS, multi-hop communication, and simulation technique are tabulated in Table 4. EETSP in [13] improved the energy efficiency and stability period of the network by optimizing the energy dissipation rate through the cluster head and secondary cluster head. EESTP needs further enhancement to deal with node mobility. ODSER in [14] achieved good energy efficiency and less end-to-end delay by employing the efficient clustering and optimized Steiner tree routing algorithms. ODSER also provided reliable communication in the event of broken links. The future enhancement required for this scheme was the use of optimized data management for resource-constrained WSN. TESEES in [15] is a multilevel heterogeneous protocol, which achieved energy saving, network lifetime, and traffic load reduction even in large-scale IoT-based WSNs. TESEES lacked QoS awareness. EEDC in [16] employed a multi-tier clustering framework to decrease the energy consumption in sensor nodes and to improve packet drop rates in scalable IoT-based WSNs. However, the limitation of the scheme is that it was unable to ensure secure communication inside network nodes.

FBCFP in [11] achieved improved energy consumption and better QoS due to the use of neuro-fuzzy rules based clustering. This method needs enhancement by considering a trust mechanism to provide secure routing. CLRP-LEACH in [18] reduced energy consumption of WSN by employing a fuzzy rule-based clustering structure and cross-layer design. The future scope required for this protocol was the addition of a lightweight security scheme. The ESEERP in [19] achieved

Table 3
Relevant literature on energy and trust based routing schemes

Protocol & Reference	Performance evaluation metrics	Advantages	Future scope
TBEERP [7]	Network life time, throughput, energy consumption and packet latency.	Improved performance in terms of network lifetime, network throughput, average energy consumption, network stability and packet latency.	To test the effectiveness of protocol in a larger network.
TEEFCA [2]	Number of alive nodes, network Lifetime, energy consumed, First node die, last node die, PDR and detection accuracy.	Improvement in power conservation, network stability and lifetime. Detected and isolated malicious nodes.	Development of intelligent based secure and energy efficient routing protocol.
PSOGA [28]	Total number of packets reaching the BS, number of alive Nodes, PDR and throughput.	Improved energy efficiency and network throughput.	To extend the work in the direction of data reduction, coupled with security.
EES-LEACH [29]	Packet delivery ratio, network life time, latency and throughput.	Higher performance in terms of the conservation of energy and secure data transmission.	To improve the performance using swarms intelligence-based optimization.
SEACDSC [30]	Stability period, network lifetime, energy usage, reliability, and CHs average trust value.	Improved network stability, energy efficiency, reliability and network lifetime.	To extend the proposed method to mobile WSNs.

very good energy efficiency and a high packet delivery ratio in WSN by employing a clustering structure, data aggregation, and sailfish optimization. The limitation of this method was that uneven energy use among the nodes and the extra work caused by threshold-based functions. SWARAM in [3] improved the packet delivery ratio and network lifetime by using the osprey-optimized clustering method. However, SWARAM needs an enhancement to be implemented in a real-time environment. The O-LEACH in [21] minimized the number of orphan nodes and enhanced the overall connectivity of the network; this ensured that more data was available at the BS, which can lead to better decision-making and quick responses in WSNs. The standard LSA suffered from poor coverage accuracy. The integration of PSO with LSA, the PSO-LSA algorithm, improved the accuracy of the solutions obtained**.** The hybrid PSO-LSA needs enhancement to handle scalability and heterogeneity.

The ESRA scheme in [22] has provided two-level security employing biometric-based authentication and data encryption using RSA and SH1. The RSA is an asymmetric encryption method that requires a large key size and creates high computation overhead and memory usage. Therefore, the ESRA scheme is not suitable for constrained WSNs. ESR in [26] provided security and reliability for data transmission, along with improved network lifetime. ESR used a lightweight threshold-based Shamir secret sharing scheme for data security. The future scope of this method was to consider multi-hop communication along with mobility. E-LEACH in [10] provided a reliable and secure connection in WSNs through an efficient key distribution and management method based on ECC. The ECC requires only a smaller key size and lower CPU and memory usage compared to RSA. E-LEACH considered a two-dimensional topology for sensor placement, which was not suitable for uneven surfaces. The MHSEER in [25] increased throughput and decreased the packet drop ratio, packet delay, energy consumption, and faulty pathways for WSN-based IIoT; even so, the suggested method has some drawbacks, such as complexity and compatibility issues. In future work, the proposed protocol will be implemented using real-world datasets for better results. EEMCM in [27] produced very high anomaly detection accuracy, along with significant enhancement in energy efficiency. However, the average end-to-end delay of EEMCM is longer than the existing methods. EEMCM used an AlexNet, a deep learning model for anomaly detection, which is computationally expensive due to its large size. TBEERP in [7] provided very good energy efficiency in heterogeneous networks and was also able to encounter malicious activities of nodes. TBEERP used a centralized clustering scheme that could affect scalability in larger networks. TEECA in [2] addressed both security and energy efficiency by employing a trust-based clustering approach. However, the trust mechanism and fuzzy rules increased the computational overhead of TEECA.

Most of the articles that are part of this survey focused on homogeneous networks for the research work; this is equal to 57.69%. The data aggregation is the process of collecting and integrating data from multiple sensor nodes into a more compact and useful form before transmitting it to the base station in WSNs. By lowering the volume of data traffic in the network, this method enhances network performance. 73.07% of papers included in this survey used the data aggregation technique for their research work. The multipath routing is used

Table 4
Summary of start of art routing protocols

Protocol & Reference	Energy efficiency	Heterogeneity	Scalability	Data aggregation	Multipath	QoS	Multi-hop	Simulator
EETSP [13]	Very Good	No	Limited	Yes	No	No	Yes	MATLAB
OEDSR [14]	Good	No	Limited	Yes	Yes	Yes	Yes	NS2.34
TESEES [15]	Very Good	Yes	High	Yes	No	No	Yes	MATLAB
EEDC [16]	Good	No	Good	Yes	No	No	Yes	MATLAB
HRP-EE [17]	Good	Yes	Limited	Yes	No	No	Yes	NS 2
EERP [9]	Good	No	Limited	Yes	No	No	Yes	Python
IEECP [5]	Good	No	High	No	No	No	Yes	MATLAB.
FBCFP [11]	Good	No	Good	No	No	Yes	Yes	MATLAB.
CLRP- LEACH [18]	Good	No	Limited	Yes	No	No	Yes	NS-2 & MATLAB
ESEERP [19]	Very Good	No	Limited	Yes	Yes	No	Yes	MATLAB.
SWARAM [3]	Very Good	Yes	Good	Yes.	No	No	No	MATLAB.
EEGT [20]	Good	Yes	Limited	Yes	Yes	No	Yes	NS2
PSO-LSA & SA-LSA [21]	Good	No	Limited	Yes	No	No	No	-
ESRA [22]	Moderate	No	Limited	No	No	Yes	Yes	MATLAB.
EES [23]	Good	Yes	Limited	Yes	No	Yes	No	NS2
E-LEACH [10]	Good	No	High	Yes	No	No	Yes	MATLAB.
OP-MDCRP [12]	Good	Yes	Good	Yes	No	Yes	Yes	MATLAB
MLRP-HTEEN-UDSP [24]	Good	Yes	Limited	Yes	Yes	Yes	Yes	NS2
MHSEER [25]	Good	No	Limited	No	No	Yes	Yes	MATLAB
ESR [26]	Good	No	Limited	Yes	No	Yes	No	NS2
EEMCM [27]	Very Good	Yes	Good	No	Yes	No	Yes	MATLAB
TBEERP [7]	Very Good	Yes	Limited	Yes	No	Yes	Yes	NS3
TEEFCA [2]	Moderate	No	Limited	No	No	Yes	Yes	MATLAB
PSOGA [28]	Good	No	Good	No	No	No	Yes	-

in WSN to achieve load balancing and is more resilient to route failures. 19.23% of papers included in this survey considered multi-path routing for data transmission. Most of the articles that are part of this survey considered multi-hop communication for the research work; this is equal to 80.76%. QoS-aware routing was considered in the research work by 46.15% of the articles that are part of this survey.

4. Open Issues and Challenges

The open issues and challenges in designing efficient routing protocols for IoT-based WSNs are discussed below.

Limited energy capacity Sensor nodes are battery-operated, and they are randomly positioned in difficult environments; in most cases they will not be replaced or recharged. Therefore, routing protocols are to be designed to utilize the energy of sensor nodes effectively to enhance the network lifetime.

Load balancing Routing protocols must be appropriately designed to distribute the network traffic effectively among all nodes to avoid the over usage of specific nodes in such a way that the network lifetime is extended.

Scalability The number of devices connected to the network grows regularly in IoT-based WSNs. The routing protocols must be designed to handle an increasing number of sensor nodes without lowering network performance.

Dynamic network conditions The topology of WSN keeps on changing due to sensor node addition, node mobility, node failure, and energy depletion. Routing protocols must be able to adapt to the changing network conditions.

Security Another crucial concern with WSN is security. The WSN infrastructure is made of small, low-cost nodes spread over a remote area; it is often impossible to prevent sensor nodes from being physically accessed by attackers (node capture). In a WSN, confidentiality and integrity of transmitted data should be ensured. Complex encryption algorithms used in conventional networks are not suitable for WSN due to the limited processing and memory capabilities of nodes; only lightweight security protocols are suitable for WSN. As a result, designing a routing protocol for WSNs that considers security, energy efficiency, and latency was a challenging task.

Delay It is an important factor for time-critical applications. In real-time applications, the important event should be reported without delay.

Fault Tolerance The sensor nodes in the WSN often fail to perform the assigned duty due to physical damage, lack of energy, or environmental interference; it is important that the WSN as a whole be able to tolerate such disturbance. The fault tolerance is the networks' ability to provide normal services even in the event of a sensor node failure.

Heterogeneity Compared to conventional wireless sensor networks, IoT-based WSNs often include a wide variety of devices or sensor nodes having varying capabilities, which include different energy levels, energy constraints, communication ranges, and data processing capabilities. Therefore, routing protocols designed for IoT-based WSNs should be capable of managing challenges with heterogeneity and mobility.

Quality of Service (QoS) is the ability of the network to deliver data reliably, timely, and efficiently in accordance with the specific application needs. In IoT-based WSNs are used for different critical applications in which maintaining a high QoS is essential in spite of constraints in the resources.

5. Conclusion and Future Directions

The integration of Wireless Sensor Networks (WSNs) with the Internet of Things (IoT) has revolutionized a wide range of industries such as environmental monitoring, agriculture, manufacturing, smart health, home automation, wildlife monitoring, and surveillance. However, energy efficiency and security are the significant challenges for WSNs. To design a routing protocol considering both energy efficiency and security is a critical challenge due to the constrained nature of nodes. This paper has provided a compact review of different existing approaches and algorithms and optimization techniques that are used to overcome the issues regarding the energy-efficient and secure routing in IoT-based WSNs. The collected papers were categorized into various routing schemes, such as the energy-efficient routing, energy and security-based routing, and energy and trust-based routing models. The article has presented an in-depth analytical summary of routing protocols, focusing on factors such as energy efficiency, heterogeneity, scalability, data aggregation, multipath, QoS, and multi-hop communication. This paper also discussed some of the open issues and challenges related to this domain. To achieve energy-efficient and secure routing in IoT-based WSN, the researchers should consider the following constraints and strategies during the design.

- Use clustering and load balancing methods for energy-efficient routing.
- Include optimization techniques to reduce the energy consumption.
- The scalability of IoT-based WSNs should be considered while designing the protocols.
- Routing protocols must be able to adjust to the dynamic network conditions.
- Efficient lightweight encryption and authentication methods must be added to achieve the security.
- Integration of advanced machine learning and block chain methods to achieve energy efficiency and security.
- Addition of trust-based methods for identifying malicious nodes.
- Routing protocols designed for IoT-based WSNs should be capable of managing challenges with heterogeneity and mobility.
- Routing protocols should control delay in time-critical applications.

References

[1] Verlecar X. N., Desai S. R., Sarcar A. and Dalal S. G. Water Res. 40. 2006. 3304. K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, “A review paper on wireless sensor network techniques in Internet of Things (IoT),” *Mater. Today Proc.*, vol. 51, pp. 161–165, 2022, doi: 10.1016/j.matpr.2021.05.067.

[2] A. R. Rajeswari, K. Kulothungan, S. Ganapathy, and A. Kannan, “Trusted energy aware cluster-based routing using fuzzy logic for WSN in IoT,” *J. Intell. Fuzzy Syst.*, vol. 40, no. 5, pp. 9197–9211, Apr. 2021, doi: 10.3233/JIFS-201633.

[3] R. Somula, Y. Cho, and B. K. Mohanta, “SWARAM: Osprey Optimization Algorithm-Based Energy-Efficient Cluster Head Selection for Wireless Sensor Network-Based Internet of Things,” *Sensors*, vol. 24, no. 2, p. 521, Jan. 2024, doi: 10.3390/s24020521.

[4] Y. B. Zikria, R. Ali, M. K. Afzal, and S. W. Kim, “Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions,” *Sensors*, vol. 21, no. 4, p. 1174, Feb. 2021, doi: 10.3390/s21041174.

[5] A. A.-H. Hassan, W. M. Shah, A.-H. H. Habeb, M. F. I. Othman, and M. N. Al-Mhiqani, “An Improved Energy-Efficient Clustering Protocol to Prolong the Lifetime of the WSN-Based IoT,” *IEEE Access*, vol. 8, pp. 200500–200517, 2020, doi: 10.1109/ACCESS.2020.3035624.

[6] J. Capella, J. Campelo, A. Bonastre, and R. Ors, “A Reference Model for Monitoring IoT WSN-Based Applications,” *Sensors*, vol. 16, no. 11, p. 1816, Oct. 2016, doi: 10.3390/s16111816.

[7] M. Ilyas *et al.*, “Trust-based energy-efficient routing protocol for Internet of things–based sensor networks,” *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 10, p. 155014772096435, Oct. 2020, doi: 10.1177/1550147720964358.

[8] R. Bharathi, S. Kannadhasan, B. Padminidevi, M. S. Maharajan, R. Nagarajan, and M. M. Tonmoy, “Predictive Model Techniques with Energy Efficiency for IoT-Based Data Transmission in Wireless Sensor Networks,” *J. Sens.*, vol. 2022, pp. 1–18, Dec. 2022, doi: 10.1155/2022/3434646.

[9] R. B. Pedditi and K. Debasis, “Energy Efficient Routing Protocol for an IoT-Based WSN System to Detect Forest Fires,” *Appl. Sci.*, vol. 13, no. 5, p. 3026, Feb. 2023, doi: 10.3390/app13053026.

[10] S. M. Hussein, J. A. López Ramos, and A. M. Ashir, “A Secure and Efficient Method to Protect Communications and Energy Consumption in IoT Wireless Sensor Networks,” *Electronics*, vol. 11, no. 17, p. 2721, Aug. 2022, doi: 10.3390/electronics11172721.

[11] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, and A. Kannan, “Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT,” *Comput. Netw.*, vol. 151, pp. 211–223, Mar. 2019, doi: 10.1016/j.comnet.2019.01.024.

[12] I. L. G and V. Kavitha, “Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment,” *Peer--Peer Netw. Appl.*, vol. 14, no. 2, pp. 821–836, Mar. 2021, doi: 10.1007/s12083-020-01038-6.

[13] A. K. Dwivedi, P. S. Mehra, O. Pal, M. N. Doja, and B. Alam, “EETSP: Energy-efficient two-stage routing protocol for wireless sensor network-assisted Internet of Things,” *Int. J. Commun. Syst.*, vol. 34, no. 17, p. e4965, Nov. 2021, doi: 10.1002/dac.4965.

[14] S. Tumula *et al.*, “An opportunistic energy-efficient dynamic self-configuration clustering algorithm in WSN-based IoT networks,” *Int. J. Commun. Syst.*, vol. 37, no. 1, p. e5633, Jan. 2024, doi: 10.1002/dac.5633.

[15] A. S. H. Abdul-Qawy *et al.*, “An enhanced energy efficient protocol for large-scale IoT-based heterogeneous WSNs,” *Sci. Afr.*, vol. 21, p. e01807, Sept. 2023, doi: 10.1016/j.sciaf.2023.e01807.

[16] D. Gupta, S. Wadhwa, S. Rani, Z. Khan, and W. Boulila, “EEDC: An Energy Efficient Data Communication Scheme Based on New Routing Approach in Wireless Sensor Networks for Future IoT Applications,” *Sensors*, vol. 23, no. 21, p. 8839, Oct. 2023, doi: 10.3390/s23218839.

[17] V.-H. Nguyen and N. D. Tan, “Voronoi diagrams and tree structures in HRP-EE: Enhancing IoT network lifespan with WSNs,” *Ad Hoc Netw.*, vol. 161, p. 103518, Aug. 2024, doi: 10.1016/j.adhoc.2024.103518.

[18] M. Nasri, A. Helali, and H. Maaref, “Energy-efficient fuzzy logic-based cross-layer hierarchical routing protocol for wireless Internet-of-Things sensor networks,” *Int. J. Commun. Syst.*, vol. 34, no. 9, p. e4808, June 2021, doi: 10.1002/dac.4808.

[19] R. Dogra, S. Rani, Kavita, J. Shafi, S. Kim, and M. F. Ijaz, “ESEERP: Enhanced Smart Energy Efficient Routing Protocol for Internet of Things in Wireless Sensor Nodes,” *Sensors*, vol. 22, no. 16, p. 6109, Aug. 2022, doi: 10.3390/s22166109.

[20] N. Duy Tan, D.-N. Nguyen, H.-N. Hoang, and T.-T.-H. Le, “EEGT: Energy Efficient Grid-Based Routing Protocol in Wireless Sensor Networks for IoT Applications,” *Computers*, vol. 12, no. 5, p. 103, May 2023, doi: 10.3390/computers12050103.

[21] G. A. Senthil, A. Raaza, and N. Kumar, “Internet of Things Energy Efficient Cluster-Based Routing Using Hybrid Particle Swarm Optimization for Wireless Sensor Network,” *Wirel. Pers. Commun.*, vol. 122, no. 3, pp. 2603–2619, Feb. 2022, doi: 10.1007/s11277-021-09015-9.

[22] J. K. Jain, “Secure and Energy-Efficient Route Adjustment Model for Internet of Things,” *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 633–657, Sept. 2019, doi: 10.1007/s11277-019-06422-x.

[23] K. Haseeb, I. Ud Din, A. Almogren, and N. Islam, “An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture,” *Sensors*, vol. 20, no. 7, p. 2081, Apr. 2020, doi: 10.3390/s20072081.

[24] R. Nagaraju *et al.*, “Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks,” *Energies*, vol. 15, no. 13, p. 4777, June 2022, doi: 10.3390/en15134777.

[25] A. Sharma, H. Babbar, S. Rani, D. K. Sah, S. Sehar, and G. Gianini, “MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT,” *Energies*, vol. 16, no. 10, p. 4198, May 2023, doi: 10.3390/en16104198.

[26] K. Haseeb, A. Almogren, N. Islam, I. Ud Din, and Z. Jan, “An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN,” *Energies*, vol. 12, no. 21, p. 4174, Nov. 2019, doi: 10.3390/en12214174.

[27] A. Thangavelu and P. Rajendran, “Energy-Efficient Secure Routing for a Sustainable Heterogeneous IoT Network Management,” *Sustainability*, vol. 16, no. 11, p. 4756, June 2024, doi: 10.3390/su16114756.

[28] M. Mishra, G. S. Gupta, and X. Gui, “Network Lifetime Improvement through Energy-Efficient Hybrid Routing Protocol for IoT Applications,” *Sensors*, vol. 21, no. 22, p. 7439, Nov. 2021, doi: 10.3390/s21227439.

[29] B. Suresh and G. Shyama Chandra Prasad, “An Energy Efficient Secure routing Scheme using LEACH protocol in WSN for IoT networks,” *Meas. Sens.*, vol. 30, p. 100883, Dec. 2023, doi: 10.1016/j.measen.2023.100883.

[30] W. Osamy, A. M. Khedr, A. A. Elsawy, P. V. Pravija Raj, and A. Aziz, “SEACDSC: secure and energy-aware clustering based on discrete sand cat swarm optimization for IoT-enabled WSN applications,” *Wirel. Netw.*, vol. 30, no. 4, pp. 2781–2800, May 2024, doi: 10.1007/s11276-024-03682-9.