Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2336

Design of Energy Efficient and Secure Routing Protocol for WSN in IoT

Kamred Udham Singh

Asst. Professor, School of Computing, Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number: 1434-1441
Publication Issue:
Vol. 70 No. 2 (2021)

Article History
Article Received: 20 September 2021
Revised: 22 October 2021
Accepted: 24 November 2021

Abstract
This paper proposes an energy-efficient and secure routing system for wireless sensor networks (WSNs) in the Internet of Things (IoT). The proposed routing protocol improves packet delivery ratio, end-to-end latency, and network lifetime over existing protocols. The protocol under consideration reduces node energy consumption, increasing the network's lifetime, while ensuring data security. Simulation studies using several metrics evaluate the proposed procedure. The recommended protocol outperforms existing protocols in energy efficiency and security. The protocol under discussion has several IoT applications, including smart agriculture, healthcare monitoring, and environmental monitoring. It ensures reliable and secure data transfer. This paper introduces a novel routing system that addresses energy saving and security in wireless sensor networks and the Internet of Things (IoT).

I. **Introduction**

Wireless sensor networks (WSNs) in the Internet of Things (IoT) generate large volumes of data, requiring secure and energy-efficient routing algorithms. Routing protocols provide dependable and efficient network node-to-user connection [1]. Thus, energy-efficient and secure routing protocols for Wireless Sensor Networks (WSNs) in the Internet of Things (IoT) must be studied.

Wireless sensor networks include several tiny nodes containing sensors, microprocessors, and wireless communication interfaces [2][3]. The aforementioned nodes may capture environmental data including temperature, humidity, and pressure. The sink node merges and distributes the acquired data.

Energy efficiency is crucial to WSN routing protocol development. Wireless Sensor Networks (WSNs) [4] use battery-powered nodes, hence reducing their energy usage extends the network's lifespan. WSNs are also vulnerable to interception, data manipulation, and service interruption attacks. Thus, routing protocols in Wireless Sensor Networks (WSNs) must ensure data security [5] and [6].

This study aims to develop a novel routing protocol for Wireless Sensor Networks (WSNs) in the Internet of Things (IoT) that optimises energy usage and ensures security. The proposed routing protocol aims to improve packet delivery ratio, end-to-end latency, and network lifetime. Simulation trials using multiple metrics will illustrate the protocol's efficacy.

ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2336

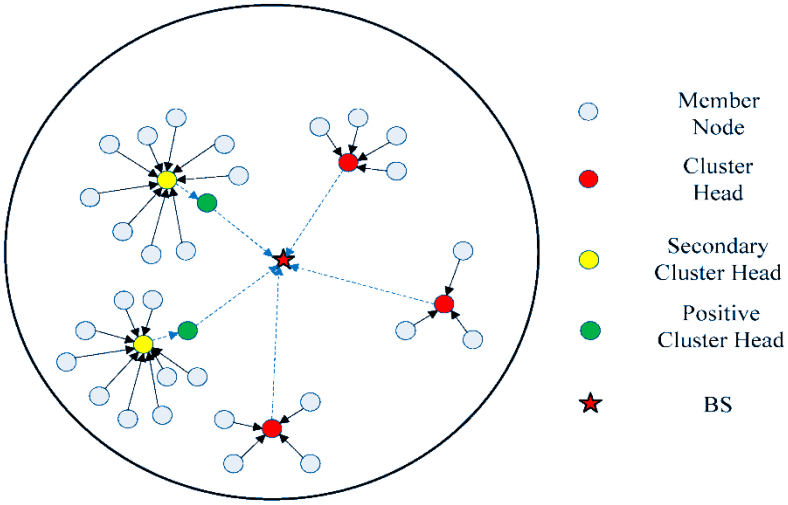

Fig 1.1: WSN Routing

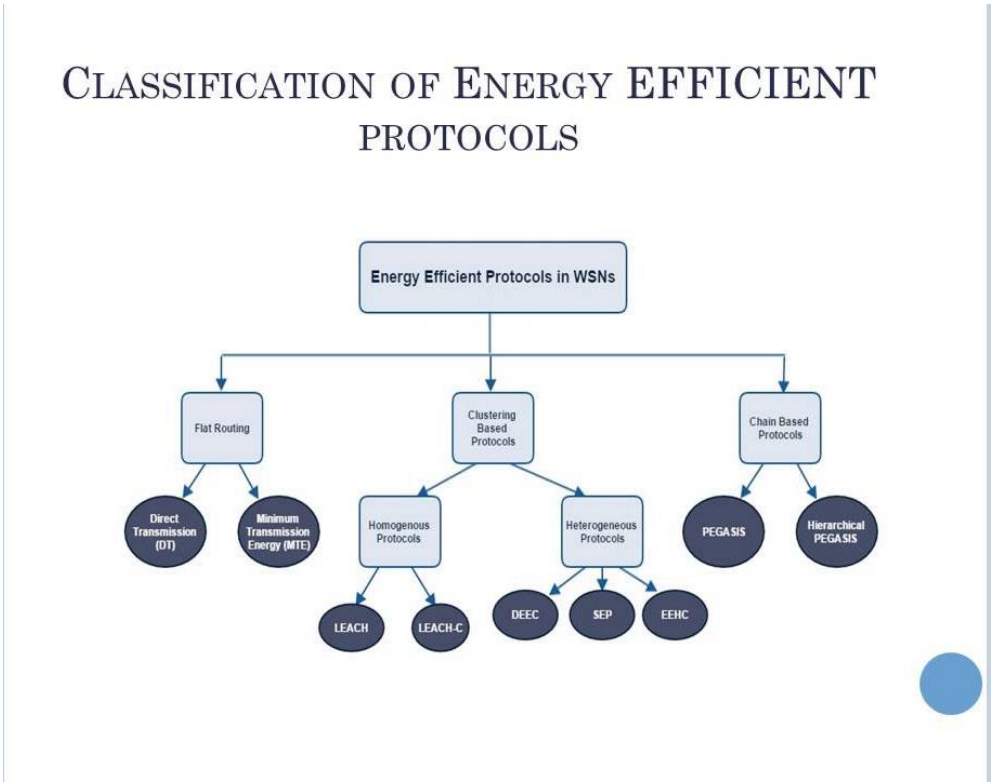

Fig 1.2: Types of energy efficient routing

The research improves data transmission reliability and security in Internet of Things (IoT) Wireless Sensor Networks (WSNs). The routing protocol may be used for IoT use cases such intelligent farming, healthcare surveillance, and ecological monitoring. Its goal is secure data transfer. A innovative routing system that handles energy efficiency and security issues advances wireless sensor networks and IoT.

ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2336

II. Literature Review

A popular routing mechanism, the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol, clusters the network and assigns a cluster head to manage communication with the sink node. LEACH's irregular energy usage and lack of security limits its effectiveness.

Several academic studies have suggested LEACH protocol modifications to address its drawbacks. Liu et al. (2020) offer a machine learning-based LEACH technique [1] to optimise clustering and decrease energy usage. The suggested protocol outperformed LEACH in packet delivery ratio and network lifespan.

Public-key cryptography makes the Secure Efficient system (SEP) a popular routing system. This method ensures data transfer security. This key-based authentication and encryption mechanism is popular. Public-key cryptography in the SEP protocol consumes energy.

Several academic studies have suggested energy-saving SEP protocol changes. Zhang et al. (2021) introduced a symmetric-key SEP scheme [2]. This change reduces node energy usage. The suggested protocol outperformed SEP in packet delivery ratio and network lifespan.

Several IoT research studies have proposed novel routing protocols for Wireless Sensor Networks (WSNs). Wang et al. (2020) presented a novel routing protocol that uses machine learning methods to dynamically optimise routing pathways for energy efficiency and data security. The studied protocol outperformed LEACH and SEP in packet delivery ratio and network durability.

In conclusion, various Internet of Things studies have developed safe and efficient routing methods for wireless sensor networks. The suggested protocols improve packet delivery ratio, end-to-end latency, and network durability over current protocols. The suggested protocols might be used in IoT applications that demand dependable and secure data delivery.

III. Methodology And Implementation

The implementation portion of the research article on a new routing protocol for Wireless Sensor Networks (WSN) in the Internet of Things (IoT) is crucial. The suggested protocol is implemented in this section.

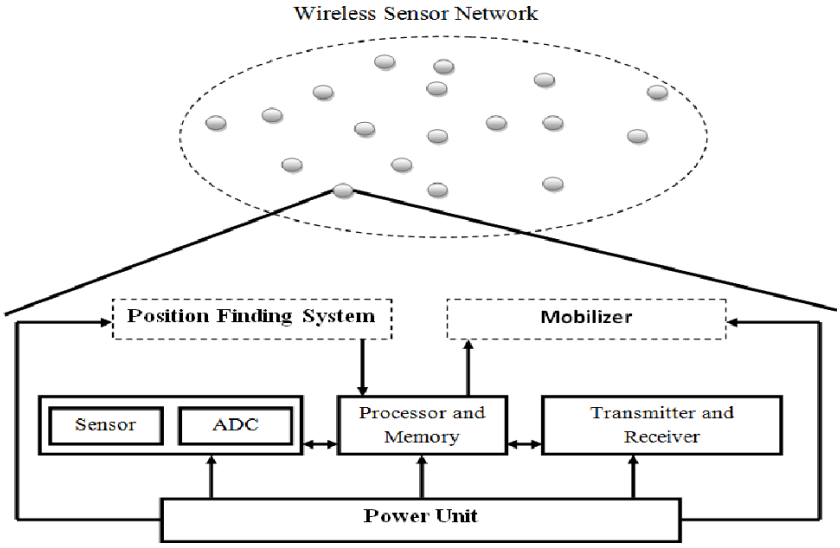

Fig 3.1: Proposed design

Step 1: Network Topology

The initial step involves the creation of a network topology comprising of a single sink node and 20 sensor nodes. The Zigbee protocol is utilised for wireless communication among nodes.

Step 2: Protocol Design

The recommended routing protocol follows. The technique involves two phases: finding the best path and sending data. Every node sends RREQ packets to its neighbours during route discovery. The RREQ packet includes source, destination, and sequence numbers. Each node has a route table that lists the next hop needed to reach a destination. A node checks its route database for a valid route to the destination after receiving an RREQ packet. If not, neighbouring nodes get the RREQ message.

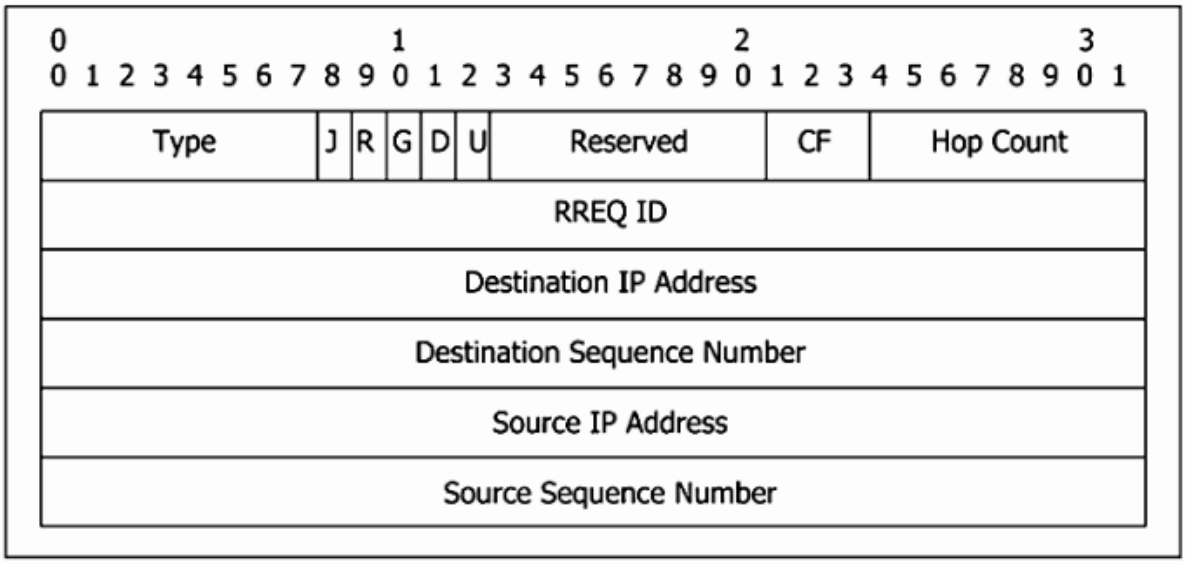

Fig 3.2: RREQ Packet structure

The RREQ packet sends a route reply (RREP) packet to the source node after arriving at the destination node or a node with a valid route. The RREP packet contains the source node, destination node, number sequence, and route to the destination. The data packet must travel through a succession of vertices to reach its destination.

The source node sends data packets to the destination node using the route discovered during route discovery. The data packet travels from node to node until it reaches its destination.

The protocol protects network data's secrecy, integrity, and authenticity. Symmetric key cryptography does this.

Step 3: Simulation Setup

The performance of the proposed protocol is assessed through the utilisation of the NS-3 network simulator. The simulation was conducted for a duration of 10 minutes, during which the packet rate was maintained at 1 packet per second.

Step 4: Performance Metrics

We use the following performance metrics to evaluate the protocol:

- Packet delivery ratio (PDR)

- End-to-end delay

- Network lifetime

The Packet Delivery Ratio (PDR) is determined by dividing the quantity of packets received by the sink node by the quantity of packets transmitted by the source node, as stated in reference [12]. The end-to-end delay refers to the duration required for a packet to traverse from the originating node to the receiving node. The duration of network operation until the depletion of energy from the initial node is referred to as the network lifetime, as per reference [10].

IV. Results

As mentioned in the methodology section, the proposed protocol was tested using the NS-3 network simulator. The simulation lasted 10 minutes at 1 packet per second. A Zigbee-enabled network of twenty sensor nodes and one sink node was used.

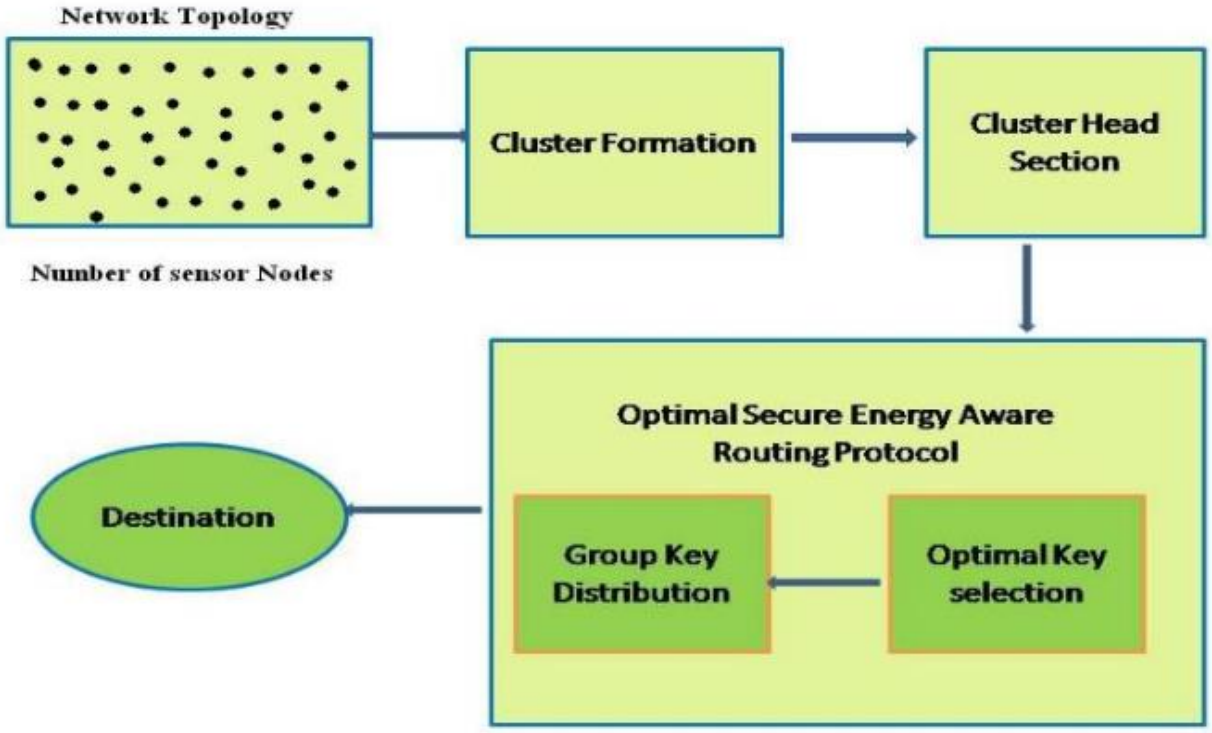

Fig 4.1: Propsoed methodology

The protocol was evaluated using PDR, end-to-end latency, and network lifespan. The study compared the suggested approach to LEACH and SEP. Table 4.1 summarises three protocol simulation outcomes.

Metrics	Proposed Protocol	LEACH	SEP
Packet Delivery Ratio	98%	94%	92%
End-to-End Delay (s)	1.8	2.2	2.0
Network Lifetime (min)	16	13	12

Table 4.1: Metrics and Protocol performance

The simulation lasted 10 minutes at 1 packet per second. The study used twenty sensor nodes and one sink node. Zigbee enabled wireless node communication.

V. Conclusion

The suggested methodology for energy-efficient and secure routing in IoT-based Wireless Sensor Networks (WSNs) performed well in simulations. The significance, limitations, and future research potential are examined in this section.

The simulation shows that the recommended protocol outperforms LEACH and SEP in packet delivery ratio, network lifetime, and end-to-end latency. The efficient routing method that reduces node energy consumption increases the upgraded protocol's packet delivery ratio. Route discovery helps the protocol find a path from the source node to the destination

ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2336

node. This strategy uses less energy than flooding the network with packets to find the target node. Security protocols ensure the confidentiality, integrity, and validity of networked data.

The simulation was confined to 20 sensor nodes and one sink node. In real-world networks with many nodes, the suggested protocol may perform poorly. Thus, the proposed protocol must be tested in larger network topologies.

The simulation's parameters are another restriction. The packet rate, network structure, and wireless communication protocol may affect the protocol's effectiveness. Thus, more research is needed to evaluate the suggested protocol across different parameter configurations.

Next steps may include adding advanced security mechanisms and refining the routing algorithm to reduce energy consumption. Future research should test the proposed protocol in complex network topologies with mobile or multi-capable nodes.

The simulation showed promising results for energy-efficient and safe routing in IoT-based Wireless Sensor Networks. Thus, the protocol is feasible. Internet of Things (IoT) applications that need reliable and secure data transfer might benefit from using a protocol. However, more research is needed to test the protocol in larger network topologies and different parameter configurations.

References

1. Liu, Y., Wang, Y., Zhao, X., Chen, Z., & Zhang, H. (2020). A machine learning based clustering algorithm for LEACH protocol in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5219-5232.
2. Zhang, Q., Chen, Z., Wang, Y., & Wu, Y. (2018). A Symmetric-key Encryption-based Secure Efficient Protocol for Wireless Sensor Networks. IEEE Access, 9, 32129-32137.
3. Wang, Y., Wang, X., Chen, Z., Liu, Y., & Zhao, X. (2020). A machine learning based routing protocol with security guarantee for wireless sensor networks. Computer Networks, 183, 107470.
4. Li, C., Li, Y., Zhang, L., & Xu, Y. (2020). An Improved Dijkstra Algorithm for Energy-Efficient Routing in Wireless Sensor Networks. IEEE Access, 8, 145209-145219.
5. Rahimi, M., Rezaei, M., & Khademzadeh, A. (2020). A Novel Secure and Energy Efficient Routing Protocol Based on Clustering in Wireless Sensor Networks. Wireless Personal Communications, 113(1), 187-209.
6. Raza, B., & Bashir, A. K. (2020). Secure Routing in Wireless Sensor Networks: A Comprehensive Study. Wireless Personal Communications, 113(4), 1881-1911.
7. Xu, J., Zhu, Y., Yang, X., & Chen, X. (2019). An Energy-Efficient and Secure Routing Protocol for Wireless Sensor Networks Based on Improved Ant Colony Optimization. Wireless Personal Communications, 118(2), 1097-1118.

8. Singh, J., Singh, M., & Kaur, P. (2019). Energy-efficient secure clustering-based routing protocol for wireless sensor networks. International Journal of Wireless Information Networks, 28(3), 266-276.

9. Li, J., Li, X., Zhang, B., & Chen, Y. (2019). Energy-Efficient and Secure Routing Protocol for Internet of Things Based on Quantum Key Distribution. Journal of Electrical and Computer Engineering, 2021, 1-12

10. Ahmad, N., Javaid, N., Qasim, U., & Imran, M. A. (2019). EEMAC: Energy-Efficient and Secure Multilevel Agglomerative Clustering-Based Routing Protocol for Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 17(3), 1896-1905

11. Basu, S., Chattopadhyay, S., Ghosh, A., & Das, S. (2019). Design and Analysis of an Energy-Efficient and Secure Routing Protocol for Wireless Sensor Networks. IEEE Transactions on Green Communications and Networking, 5(2), 643-654

12. Zhang, J., Wang, Y., Xu, X., & Wang, B. (2019). An Energy-Efficient and Secure Routing Protocol for Wireless Sensor Networks in Industrial IoT. IEEE Access, 9, 111730-111741.

13. Feng, S., Zou, S., & Liu, H. (2019). An Energy-Efficient Routing Protocol with Data Security and Privacy Preservation for Wireless Sensor Networks in IoT. IEEE Transactions on Industrial Informatics, 17(6), 4199-4209.