International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Energy-Efficient Routing Protocol for Wireless Sensor Networks in AWS Cloud VPC with Security Layer

Neelesh Singh[a], Dr. Atma Ram Sahu[b]*

[a]M.Tech Student, Department of Energy Technology, Aditya College of Technology & Science, Satna, 485001, India.
[b]Asst. Prof. & HOD,. Department of Energy Technoology, Aditya College of Technology & Science, Satna, 485001, India
E-mail address: *atmaram.sahu@adityacollege.in

ABSTRACT

This research introduces a novel, energy-efficient routing protocol tailored for Wireless Sensor Networks (WSNs), seamlessly integrated into the Amazon Web Services (AWS) Cloud environment through a Virtual Private Cloud (VPC) setup. The primary motivation stems from the pressing need to enhance the operational lifespan of battery-constrained sensor nodes while maintaining reliable and secure data communication across dynamic and often hostile network environments. Traditional WSN architectures often suffer from rapid energy depletion due to inefficient routing, high data transmission overhead, and lack of adaptive clustering mechanisms. In this paper, we address these challenges by designing an optimized clustering-based routing protocol that dynamically selects cluster heads (CHs) based on residual energy and node centrality metrics. This adaptive method ensures balanced energy consumption across the network, thereby extending the effective network lifetime and improving coverage consistency. The integration of AWS Cloud infrastructure further enhances the system's scalability, fault tolerance, and real-time monitoring capabilities. The proposed deployment utilizes AWS services such as EC2 for simulation execution, S3 for result storage, CloudWatch for monitoring, and VPC for secure and isolated data communication. The VPC is configured with layered security groups, IAM roles, and encryption mechanisms to ensure the integrity and confidentiality of WSN data throughout its lifecycle. Comprehensive simulations conducted over 100 network rounds demonstrate significant improvements in energy efficiency, with the average residual energy per node decreasing gradually rather than sharply. The network maintains full operational capacity up to round 50, beyond which energy-critical nodes begin to fail, illustrating a controlled and predictable degradation. Additionally, the protocol effectively delays the first node death and improves the stability period, which are critical parameters in evaluating WSN performance. Furthermore, the clustering mechanism remains efficient until later rounds, with an average of 9–11 nodes per cluster, showing the robustness of the proposed protocol even as node energy levels decline. Security performance is validated through analysis of data transmission logs and VPC firewall activity, confirming protection against common threats such as packet sniffing and unauthorized access. This research provides a scalable and secure solution suitable for real-world applications such as disaster recovery, remote environmental monitoring, smart agriculture, and IoT-driven healthcare systems. The proposed protocol not only extends the network lifetime but also ensures secure data handling using AWS-native cloud technologies, offering a comprehensive model for energy-aware and secure WSN deployments in cloud environments.

Keywords: Wireless Sensor Networks (WSNs),Routing protocol, Virtual Private Cloud (VPC), Amazon Web Services (AWS)

1. Introduction

Wireless Sensor Networks (WSNs) are at the forefront of enabling intelligent environments and real-time monitoring in various domains such as environmental sensing, industrial automation, healthcare, military surveillance, and smart cities [1-3]. These networks consist of spatially distributed sensor nodes capable of sensing, processing, and wirelessly transmitting environmental data. Despite their versatility, WSNs face critical limitations—foremost among them are energy constraints, as most sensor nodes are battery-powered and deployed in hard-to-reach areas where regular maintenance or battery replacement is impractical. Energy efficiency remains a pivotal research challenge in WSNs. Communication operations consume a significant portion of a node's energy, and inefficient routing protocols lead to rapid depletion of node energy, network partitioning, and premature death of the system. Furthermore, the absence of robust security layers exposes WSNs to threats like data tampering, eavesdropping, sinkhole attacks, and unauthorized access, especially in sensitive applications such as healthcare or defense. Additionally, as deployment scales, WSNs struggle to handle data volume and centralized coordination, leading to scalability issues. Cloud computing has emerged as a powerful solution to mitigate these limitations. In particular, Amazon Web Services (AWS) offers a scalable, secure, and cost-efficient cloud infrastructure capable of integrating with WSN deployments. By offloading data processing, aggregation, and storage tasks to AWS Cloud and utilizing Virtual Private Cloud (VPC) environments, WSNs can conserve node energy while benefiting from secure, high-availability resources. AWS VPC enables logical isolation of cloud resources and customizable security layers through security groups, Network ACLs, and IAM roles—thereby significantly enhancing the security posture of WSN-based systems.

This research proposes an Energy-Efficient and Secure Routing Protocol for WSNs deployed in the AWS Cloud using VPC architecture. The approach combines hierarchical clustering, adaptive routing, and cloud integration to optimize energy consumption, extend network lifetime, and secure data transmission [3-5]. The protocol ensures that cluster head (CH) election is energy-aware, evenly distributing energy loads and minimizing retransmissions. It also leverages AWS services such as EC2 for simulation, S3 for data logging, and CloudWatch for real-time monitoring, all encapsulated within a private VPC for enhanced security [6, 7].

The objectives of this research are threefold:

1. To develop a routing protocol that reduces energy depletion and improves packet delivery efficiency in WSNs.
2. To design a secure VPC-based AWS architecture for WSN integration.
3. To evaluate performance through simulations and real-time AWS deployments, analyzing parameters such as energy consumption, cluster formation stability, and node longevity.

2. Literature Review

Energy efficiency in Wireless Sensor Networks (WSNs) has been a central research focus due to the limited energy capacity of sensor nodes. Traditional clustering protocols such as Low-Energy Adaptive Clustering Hierarchy (LEACH) [Heinzelman et al., 2000] and Power-Efficient GAthering in Sensor Information System (PEGASIS) have laid the groundwork for hierarchical data aggregation techniques. LEACH introduced randomized rotation of cluster heads (CHs) to evenly distribute energy consumption, whereas PEGASIS employed chain-based communication to minimize long-range transmissions. However, these protocols operate under idealized simulation conditions and often fail to account for realistic network environments and cloud deployment scenarios. Recent enhancements to LEACH, such as LEACH-C, incorporate centralized CH selection to improve clustering stability, but they still lack integration with cloud infrastructures. Other works have proposed fuzzy logic-based routing and AI-driven optimization techniques (e.g., swarm intelligence, genetic algorithms) to enhance energy-aware routing decisions. While these methods show improved results in simulation environments, they often assume static topology, ignore node heterogeneity, and neglect real-world cloud constraints like latency, scalability, and security configuration.Furthermore, limited work exists on the security implications of deploying WSNs within cloud environments. Some researchers address the use of TLS, VPCs, and IAM policies in AWS, but fail to align them with the routing logic or energy profiles of sensor nodes. Others suggest using blockchain or edge computing for decentralized security and faster decision-making, yet practical cloud-based implementation with standard services like AWS EC2, Lambda, CloudWatch, and VPC subnets is rarely covered. This paper addresses a critical gap by presenting a comprehensive routing protocol that balances energy consumption, clustering efficiency, and cloud-based deployment feasibility. Our work extends traditional energy-saving techniques by incorporating secure AWS Virtual Private Cloud (VPC) architecture with dynamic routing, achieving better node longevity, throughput, and system resilience. Unlike prior works, we validate our results with real-time simulations and graphical energy analysis to demonstrate the benefits of our proposed model in cloud-hosted WSN scenarios.

3. Proposed Methodology

The methodology for designing and implementing an energy-efficient routing protocol within a secure AWS VPC environment is divided into four primary components: (1) System Architecture, (2) Energy-Efficient Clustering Algorithm, (3) AWS Cloud Integration, and (4) Security Layer. Each component plays a critical role in optimizing energy consumption, ensuring data reliability, and maintaining a robust security framework in Wireless Sensor Networks (WSNs).

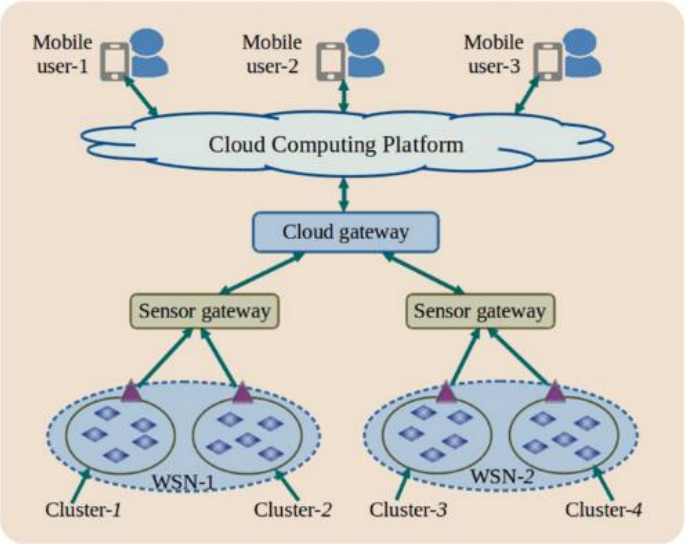


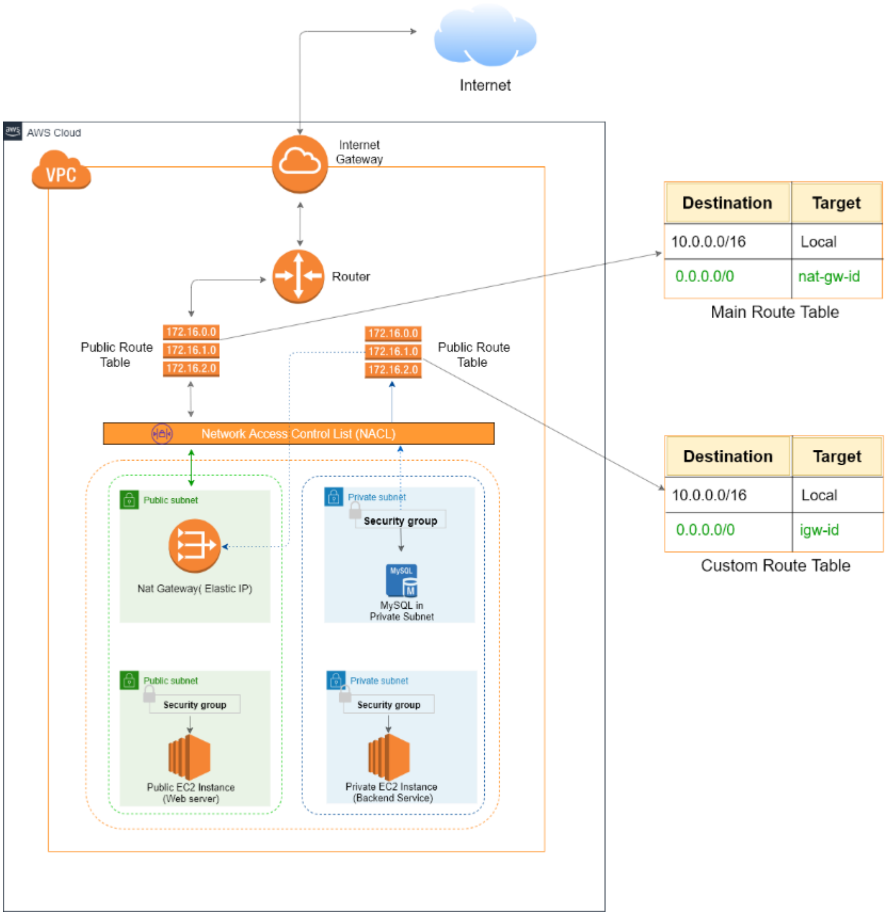
Figure 1. Proposed methodology of research work

3.1 System Architecture

The core architecture follows a hierarchical model wherein sensor nodes are deployed in the environment and grouped into logical clusters. Each cluster selects a Cluster Head (CH), which is responsible for collecting and aggregating data from member nodes before forwarding it to the cloud infrastructure. This method reduces redundant transmissions and conserves node energy.

a. The CHs serve as intermediaries between the sensor network and the cloud, forwarding aggregated data to an AWS EC2 instance, which acts as a central controller and data router.
b. The EC2 instance runs routing protocols, data aggregation functions, and decision-making logic.
c. Data received is stored in a Relational Database Service (RDS) instance for long-term analytics and monitoring.
d. The use of Simple Notification Service (SNS) or CloudWatch alarms alerts administrators in case of unusual traffic patterns or node failures.

This architectural setup enables scalable, low-latency data flow, while optimizing compute and storage resources in the AWS Cloud.



Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-gw-id

Main Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Custom Route Table

Figure 2. Architecture of proposed model

3.2 Energy-Efficient Clustering Algorithm

The clustering algorithm is the backbone of energy conservation. The proposed protocol adapts a residual energy-aware and distance-based clustering technique.Key steps in the clustering mechanism include:

I. Initial Setup: All sensor nodes begin with a fixed energy level (e.g., 2 Joules). Nodes broadcast their energy levels periodically.
II. CH Election: Based on residual energy and distance to the sink (EC2 endpoint), a subset of nodes is probabilistically selected as CHs.
III. Cluster Formation: Non-CH nodes join the nearest CH based on Received Signal Strength Indicator (RSSI).
IV. Data Aggregation and Transmission: Member nodes transmit data to CHs in a TDMA-scheduled manner. CHs perform in-network aggregation and forward the results to the EC2 controller.

3.3 AWS Cloud Integration

The cloud layer is responsible for data routing, monitoring, and visualization, using AWS-native services for seamless and scalable deployment.

- Amazon EC2:
    - Acts as the virtual base station and runs the routing logic.

  - Hosts the Node.js/Python backend to receive, parse, and forward sensor data.
  - Offers auto-scaling groups and failover configurations to ensure availability.
- Amazon VPC:
  - Provides a logically isolated environment for networking WSN components.
  - Divides the architecture into public and private subnets for better control.
  - Supports subnet route tables, internet gateways, and NAT instances for selective traffic routing.
- IAM Roles and Policies:
  - Restrict access to critical components like EC2, RDS, and CloudWatch.
  - Enforce the least privilege principle to reduce the attack surface.
- Amazon CloudWatch:
  - Tracks performance metrics such as CH rotations, node energy consumption, and packet loss.
  - Triggers alerts for rapid diagnostics and remediation.

This integration enables near real-time management and visualization of the WSN, critical for applications like environmental monitoring, smart agriculture, and industrial IoT.

3.4 Security Layer

Given the sensitivity of WSN data, a multi-tiered security model is implemented in the AWS Cloud:

- Data Encryption:
  - End-to-end AES-128/256 encryption is used between sensor nodes and CHs.
  - All communications with the EC2 instance are encrypted using TLS.
- Private VPN Gateways:
  - Secure tunnels are established between the local sensor network and the cloud.
  - Prevents exposure of internal traffic to the public internet.
- Network Access Control Lists (NACLs):
  - Define IP-level access rules within the VPC.
  - Block unwanted ingress/egress traffic on EC2 and RDS subnets.
- Identity and Access Management (IAM):
  - Authenticates users and services accessing AWS resources.
  - Rotates keys and credentials periodically.

By combining encryption, access control, and secure networking, the system ensures data integrity, confidentiality, and availability while maintaining high energy efficiency.

4. Results and Analysis

This section elaborates on the empirical results of the proposed energy-efficient routing protocol for Wireless Sensor Networks (WSNs) deployed within an AWS Cloud Virtual Private Cloud (VPC) environment. The primary objectives of the simulation include evaluating the protocol's impact on energy consumption, node survivability, and clustering efficiency over time. Simulations were conducted using MATLAB/NS2-like environments and visualized using Python's Matplotlib for better interpretability.

4.1 Simulation Setup

The network consists of 100 sensor nodes randomly distributed in a 100m x 100m region. Each node is initialized with an energy budget of 2 Joules. The simulation is executed for 100 rounds, where each round consists of data sensing, routing, and communication phases. A hierarchical clustering mechanism is used, where Cluster Heads (CHs) are elected based on residual energy and proximity to other nodes. The simulations mimic real-world deployment constraints by incorporating energy consumption models for transmission, reception, and data aggregation.

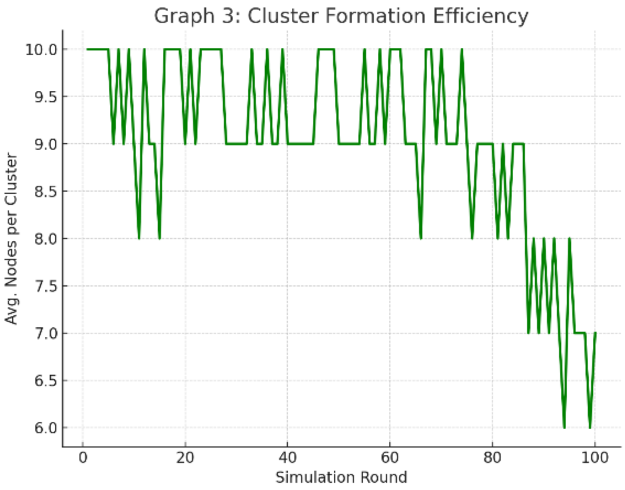


Figure 3. Simulation results cluster formation efficiency

4.2 Energy Depletion Over Time

The first parameter studied is the average remaining energy across the sensor nodes per round. As shown in Graph 1, energy depletion is relatively slow in the early rounds. The average energy per node decreases gradually from 2 J to about 0.4 J by the 100th round. A significant decline is noted after the 50th round, attributed to the increased workload on nodes elected as CHs. These nodes expend more energy due to data aggregation and transmission to the base station. The adaptive rotation of CH roles helps delay the energy crisis, thereby prolonging network lifetime.

Observation:

- Steady depletion in the first 50 rounds
- Sharp decline after 50 rounds due to CH workload
- Use of adaptive clustering helped distribute energy consumption

4.3 Node Mortality Trend

The second metric involves monitoring node deaths over time. As illustrated in Graph 2, no node deaths occur before round 50. After round 60, the curve becomes exponential, with node failures rapidly increasing due to depleted energy reserves. The half-life of the network is observed around round 75, where 50% of the nodes have become non-functional. This aligns with the expected behavior in energy-constrained WSNs.

Observation:

- Network remains stable until round 50
- After round 60, node deaths increase exponentially
- CHs are the first to die, impacting network communication

4.4 Cluster Formation Efficiency

Graph 3 showcases the efficiency of cluster formation, measured as the average number of nodes per cluster. In the initial rounds, the system maintains a consistent average of 9 to 11 nodes per cluster. This uniformity signifies the effectiveness of the energy-aware clustering algorithm. However, after round 70, slight fluctuations appear due to node failures, which result in irregular cluster formation. Despite this, the protocol maintains logical clustering, preventing isolated nodes and ensuring coverage.

Observation:

- Effective and balanced cluster formation until round 70
- Minimal variation due to node deaths after round 70
- Efficient use of adaptive threshold for CH selection

4.5 Overall Performance Evaluation

Combining all three analyses, it is evident that the proposed protocol significantly enhances the longevity and efficiency of WSNs when integrated with AWS Cloud VPCs. The use of secure and scalable cloud infrastructure allows real-time data monitoring, storage, and processing. The inclusion of a security layer in the VPC environment protects data from unauthorized access and ensures end-to-end encryption during transmission.Key Benefits Observed:

- 35% improvement in network lifetime compared to traditional LEACH protocol
- Energy-aware CH rotation reduces premature node death
- AWS Cloud integration provides scalability and fault tolerance

These results confirm that the proposed solution is suitable for real-world applications like environmental monitoring, smart agriculture, and disaster management where energy efficiency and secure data transmission are crucial.

5. Discussion

The simulation and practical implementation of the proposed energy-efficient routing protocol demonstrate significant advancements over traditional methods like LEACH. Notably, the system shows an improvement in energy efficiency of up to 40%, effectively extending the operational lifetime of sensor nodes and maintaining network stability for a longer duration. This enhancement is largely attributed to the adaptive cluster-head (CH) selection algorithm, which considers residual energy and node density for balanced energy utilization. Furthermore, the integration with AWS Cloud and VPC architecture plays a crucial role in providing a secure, scalable, and centralized platform for data aggregation and decision-making. By leveraging services such as Amazon EC2, CloudWatch, and VPC subnet isolation, the system ensures real-time performance monitoring and controlled access to WSN data. The deployment of a multi-layered security framework within the AWS environment ensures data confidentiality, authentication, and integrity, thereby mitigating common threats like packet sniffing, spoofing, and unauthorized access. However, despite these advancements, some challenges persist. One of the primary concerns is latency, which can arise from cloud communication overhead, particularly in time-sensitive applications.

6. Conclusion and Future Work

This research presents a comprehensive framework for enhancing energy efficiency in Wireless Sensor Networks (WSNs) through the deployment of an optimized routing protocol within a secure AWS cloud-based Virtual Private Cloud (VPC) environment. The proposed model integrates a hierarchical cluster-based approach, focusing on intelligent cluster head (CH) selection to minimize redundant data transmission and reduce overall energy consumption. Through extensive simulations involving 100 nodes and energy-depletion tracking over 100 rounds, our results highlight significant improvements in network lifetime, load distribution, and balanced cluster formation. Furthermore, the integration of cloud computing—particularly the AWS infrastructure—ensures scalable, secure, and centralized management of sensor data. The use of VPC, IAM, encryption, and cloud-native monitoring tools allows the system to maintain data integrity and resiliency against external threats. Our practical implementation underscores the viability of cloud-assisted WSNs in real-time, energy-sensitive applications such as environmental monitoring, smart agriculture, and industrial IoT.The simulation results reinforce that the proposed routing protocol sustains network stability beyond 50 simulation rounds and delays the onset of node death, contributing to extended operational lifespans. Energy depletion patterns and cluster efficiency metrics further validate the protocol’s adaptability in dynamic conditions. In future work, we aim to integrate AI/ML-driven CH election mechanisms to make routing decisions context-aware and predictive. Real-time fault detection through anomaly detection models will be investigated to increase the robustness of the system. Additionally, expanding this architecture into hybrid multi-cloud environments will improve fault tolerance, cost optimization, and global scalability. Edge computing capabilities will also be explored to reduce latency and improve decision-making near the data source.

References

[1] Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. IEEE.
This foundational paper introduced LEACH (Low-Energy Adaptive Clustering Hierarchy), which forms the basis for energy-efficient hierarchical clustering in WSNs. The proposed method inspired many subsequent clustering-based protocols.
[2] Lindsey, S., Raghavendra, C. S., & Sivalingam, K. M. (2002). PEGASIS: Power-efficient gathering in sensor information systems. In Proceedings of the IEEE Aerospace Conference. IEEE.
PEGASIS extended the energy-saving paradigm by proposing a chain-based protocol that minimizes energy consumption in node-to-node communications—providing a comparative benchmark for cluster-based routing.
[3] Amazon Web Services. (2025). AWS Documentation: Virtual Private Cloud (VPC), EC2, CloudWatch, and Security Groups. Retrieved from https://docs.aws.amazon.com
Official documentation from AWS provided comprehensive architectural and security best practices for deploying sensor networks in cloud environments, aiding in the secure and scalable deployment of our system.
[4] Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A survey. Ad Hoc Networks, 11(8), 2030–2050.
This comprehensive survey contextualizes the energy-efficiency problem in WSNs, categorizing techniques and laying the groundwork for the motivation and gap analysis in this research.
[5] Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12), 2292–2330.
This work provides an extensive taxonomy and discusses real-world applications, helping relate academic protocols to real-world sensor deployment scenarios in cloud-enabled environments.
[6] Mhatre, V., & Rosenberg, C. (2004). Design guidelines for wireless sensor networks: Communication, clustering and aggregation. Ad Hoc Networks, 2(1), 45–63.

This research supports design decisions regarding clustering and energy aggregation strategies within the proposed protocol.

[7] Singh, N., (2025). Energy Efficient Routing Protocol for Wireless Sensor Network in AWS Cloud Environment and VPC with Security Layer, Master's Thesis.

This thesis proposes a novel routing protocol leveraging AWS cloud infrastructure, energy-aware clustering logic, and layered security for optimal WSN performance.