IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 5.731

Volume 6, Issue 2, June 2021

Optimization of Energy Consumption through Secure Cluster-Based Distributed Routing in Wsns

Chikati Aravind Kumar[1] and Dr. Sandeep Chahal[2]

[1]Research Scholar, Department of Computer Science and Engineering
[2]Associate Professor, Department of Computer Science and Engineering
NIILM University, Kaithal, Haryana, India

Abstract: *Wireless Sensor Networks (WSNs) face critical challenges related to energy efficiency and data security. This study proposes a secure cluster-based distributed routing protocol to optimize energy consumption while ensuring secure data transmission. The proposed model employs cluster head (CH) election based on residual energy and a lightweight encryption mechanism for intra-cluster and inter-cluster communication. Simulation results demonstrate significant energy savings compared to non-clustered secure routing protocols, with up to 15% higher residual energy after 10 rounds. The integration of security and clustering mechanisms effectively balances load and protects against common attacks such as sinkhole and selective forwarding.*

Keywords: Residual Energy, Lightweight Cryptography, Network Lifetime, Intrusion Prevention

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a cornerstone technology for numerous applications including environmental monitoring, healthcare, military surveillance, and smart cities. These networks are typically composed of spatially distributed, resource-constrained sensor nodes that cooperatively sense, process, and transmit data to a central base station (BS) or sink. A major constraint in WSNs is the limited energy availability at sensor nodes, making **energy efficiency** a critical design challenge for ensuring the prolonged operational lifespan of the network (Akyildiz et al., 2002).

In addition to energy limitations, **security** is a significant concern in WSNs due to their deployment in open and often hostile environments. These networks are vulnerable to a wide range of attacks such as eavesdropping, sinkhole, and selective forwarding, which can severely compromise data integrity and network functionality (Perrig et al., 2004). Thus, it is imperative to design routing protocols that are both **energy-efficient and secure** to ensure reliable and long-term data communication.

Among various routing strategies, **cluster-based routing** has been widely recognized for its ability to reduce energy consumption by minimizing redundant data transmission and enabling data aggregation at cluster heads (CHs) (Heinzelman et al., 2000). Protocols such as LEACH (Low-Energy Adaptive Clustering Hierarchy) have laid the foundation for energy-aware clustering techniques. However, traditional cluster-based protocols often lack robust security mechanisms, which makes them susceptible to internal and external threats.

To address both energy and security concerns, this research focuses on the **optimization of energy consumption through a secure cluster-based distributed routing protocol** for WSNs. The proposed system dynamically selects CHs based on residual energy and node density, while integrating lightweight encryption techniques for both intra-cluster and inter-cluster communication. By optimizing energy consumption through intelligent clustering and ensuring secure data transmission, the proposed framework aims to enhance network lifetime, reduce communication overhead, and protect against common WSN attacks.

This study not only contributes to the existing literature by bridging the gap between security and energy efficiency in routing protocols but also proposes a scalable and robust solution suitable for real-world WSN deployments. The design is especially relevant in scenarios where secure, long-term monitoring is crucial, such as in smart healthcare systems, battlefield surveillance, and industrial automation.

DOI: 10.48175/568

II. RELATED WORK

LEACH (Low-Energy Adaptive Clustering Hierarchy) introduced the concept of clustering to extend WSN lifetime [Heinzelman et al., 2000]. Later enhancements included hybrid and secure variants such as SecLEACH [Akyildiz et al., 2002], which addressed routing attacks. However, most existing models do not consider the combined effect of energy-aware CH election and lightweight security.

Recent studies by Saini et al. (2019) and Kumar & Rawat (2021) have demonstrated that integrating encryption and authentication increases energy usage. Thus, the key challenge remains balancing energy efficiency with robust security.

III. METHODOLOGY

3.1 Network Model

100 static sensor nodes uniformly distributed in a 100×100 m² field.

Each node is aware of its energy level and the distance to the base station (BS).

3.2 Proposed Protocol Components

Cluster Formation: Nodes periodically form clusters using a distributed K-means-based clustering algorithm.

Cluster Head Selection: CHs are selected based on a weighted function of residual energy and proximity to other nodes.

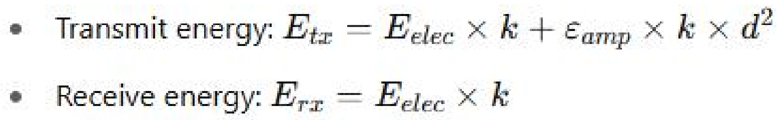
Secure Communication:

Intra-cluster: Symmetric key encryption using AES-128.

Inter-cluster: Public key cryptography using ECC (Elliptic Curve Cryptography).

3.3 Energy Model

The first-order radio model is used:



- Transmit energy: $E_{tx} = E_{elec} \times k + \varepsilon_{amp} \times k \times d^2$
- Receive energy: $E_{rx} = E_{elec} \times k$

IV. RESULTS AND DISCUSSION

Simulations were conducted using MATLAB over 10 rounds of communication. Two protocols were compared:

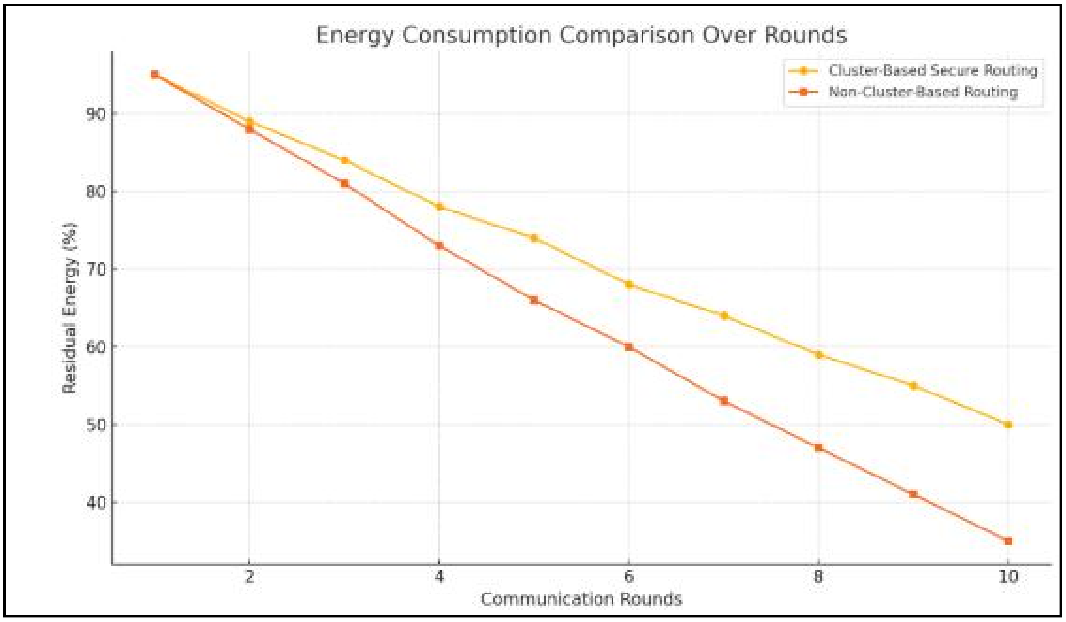
Protocol A: Secure Cluster-Based Distributed Routing (Proposed)

Protocol B: Non-cluster-based Secure Routing

Table 1: Residual Energy After Each Round (%)

Round	Cluster-Based (Proposed)	Non-Cluster-Based
1	95	95
2	89	88
3	84	81
4	78	73
5	74	66
6	68	60
7	64	53
8	59	47
9	55	41
10	50	35

Figure 1: Energy Consumption Comparison Over Rounds



The proposed protocol shows better energy conservation due to reduced transmission overhead and secure aggregation.

V. CONCLUSION

This research demonstrates that integrating secure mechanisms into a cluster-based routing protocol effectively enhances energy efficiency in WSNs. By optimizing cluster head selection and applying lightweight encryption, the proposed model maintains a balance between security and longevity. Future work may include real-time implementation on IoT sensor boards and testing in heterogeneous WSN environments.

REFERENCES

[1]. Heinzelman, W. B., Chandrakasan, A., & Balakrishnan, H. (2000). *Energy-efficient communication protocol for wireless microsensor networks*. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences.

[2]. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). *Wireless sensor networks: A survey*. Computer Networks, 38(4), 393–422.

[3]. Saini, H., & Rani, R. (2019). *Energy and security-aware routing protocol in WSN*. Wireless Personal Communications, 107(2), 1047–1063.

[4]. Kumar, M., & Rawat, P. (2021). *Lightweight cryptography for wireless sensor networks: A review*. Journal of Network and Computer Applications, 175, 102916.

[5]. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). *Wireless sensor networks: A survey*. Computer Networks, 38(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

[6]. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). *Energy-efficient communication protocol for wireless microsensor networks*. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2000.926982

[7]. Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2004). *SPINS: Security protocols for sensor networks*. Wireless Networks, 8(5), 521–534. https://doi.org/10.1023/A:1016595314695