Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 2-B, pp. 1087–1095
DOI : 10.47974/JDMSC-2648

Performance evaluation of wireless sensor networks using adaptive clustering and homomorphic polynomial encryption schemes

Linesh Raja [$]
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

C. S. Lamba [†]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Puneet Chandra Verma [§]
Department of Bachelor of Computer Applications
Government Professional College Banas-Paithani
Pauri Garhwal 246123
Uttarakhand
India

Vishal Sharma [‡]
Honey Gochar [@]
Amity Institute of Information Technology
Amity University Jaipur
Jaipur 303002
Rajasthan
India

[$] *E-mail:* `linesh.raja@jaipur.manipal.edu`
[†] *E-mail:* `cs.lamba@jaipur.manipal.edu`
[§] *E-mail:* `cvermapuneet@gmail.com`
[‡] *E-mail:* `er.vishu1983@gmail.com`
[@] *E-mail:* `honeygocher@outlook.com`

© Taru Publications

Shilpa Sharma [#]
Chandrashekhar Patel *
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

In the field of Wireless Sensor Networks efficient power management and secure communication is a serious challenge. This research article presents the combined approach of adaptive cluster head rotation with homomorphic polynomial cryptography to enhance performance as well as security of WSNs .The proposed methods used the Fuzzy C algorithms for clustering in consideration with distance and residual power and to provide the secure communication between the intra cluster domain, the author has proposed a symmetric homomorphic polynomial-based key distribution mechanism, which ensure robust encryption between sensor nodes and their respective cluster heads. The results show that the proposed technique significantly reduces power consumption by 52%, increases network throughput by 200.65%, and maintains all nodes alive up to 4000 rounds, with only a slight drop to 93.75% by 5000 rounds, thereby improving the network lifespan. These findings show the implications that the proposed techniques ensure the efficacy and sustainability of the Wireless Sensor Networks (WSNs).

Subject Classification: *Primary 68M250, Secondary 68M99.*

Keywords: *WSNs, IoT, LEACH, K-Means, FCM, ANOVA, Fuzzy-C.*

1. Introduction

For real-time monitoring of the Wireless Sensor Networks (WSNs) environment, sensors collect data and transmit it to the base station as shown in figure 1. WSNs are appealing due to advantages like low power consumption, low cost, and multi-function capabilities. Today, WSNs are increasingly popular in advanced technologies such as IoT, intelligent medical services, agriculture, and other industries.

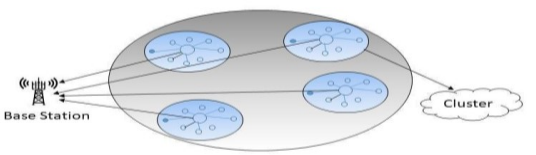

Figure 1
Wireless sensor network cluster architecture

[#] *E-mail:* **Shilpa.sharma@jaipur.manipal.edu**
* *E-mail:* **chandrashekhar.patel@jaipur.manipal.edu (Corresponding Author)**

The development of cluster head selection algorithms in wireless sensor networks has evolved from LEACH to BCSA and then to FBECS. LEACH, despite being revolutionary, has drawbacks of not considering residual energy, single-hop communication and uneven cluster formations inefficiencies. After that BCSA has issued with load distribution among sensor networks. Later Fuzzy Based Enhanced Cluster Head Selection (FBECS) improves this drawback, but it does not periodically rotate CHs, which can still lead to energy imbalances. To solve this problem this research proposes the FBATRCS protocol which improvises FBECS by including adaptive clustering with periodic CH rotation and an adaptive threshold based on average distance to the bases station. Furthermore, this work also incorporates homomorphic polynomial encryption using a symmetric key distribution mechanism for secure intra- and inter-cluster communication.

2. Related Work

Wireless Sensor Networks (WSNs) contain nodes that perform sensing and routing tasks. Since data transmission consumes significantly more energy than local processing, clustering has become a key strategy to reduce transmission overhead and extend network lifetime. LEACH was among the first protocols to introduce random rotation of Cluster Heads (CHs) for balanced energy consumption, though it lacked dynamic adaptability. To improve CH selection, Bhatti, Saeed, and Nam [1] used Fuzzy C-Means (FCM) clustering based on residual energy, SNR, and distance. Mehra, Doja, and Alam [2] proposed FBECS, applying fuzzy logic using node energy, density, and sink distance. Wan et al. [3] and Naderloo, Aghda, and Mirfakhraei [4] further used fuzzy-based techniques to reduce redundancy and enhance data relevance. While effective, these models often rely on static CH roles and do not support timely updates based on dynamic conditions. Adaptive clustering methods such as Agrawal and Pandey [5] fuzzy-based routing redistributed node associations to reduce energy gaps. Hada and Srivastava [6] and Priyadarshini and Sivakumar [7] developed dynamic CH re-election techniques, while Durugkar and Poonia [8] applied PSO for self-organizing cluster formation. However, Das, Nandi, and Roy [9] such heuristic methods may introduce computational burdens unsuitable for lightweight WSN nodes. In addition to Chaudhary, Verma, and Gupta [10] energy efficiency, ensuring secure communication is critical, as WSNs often transmit sensitive data Kokate et al. [11]. Many existing protocols overlook this aspect. Homomorphic Polynomial Encryption mathematical model offer a lightweight and efficient mechanism for securing inter-node communication with minimal computational overhead Siddamsetti et al.[12]. These methods can authenticate data integrity and prevent unauthorized access while maintaining energy efficiency Singh et al. [13]. The proposed work integrates lightweight cryptographic methods to secure WSN Goyal et al. [14]. This approach ensures balanced energy consumption and secure, reliable communication, making it

ideal for real-time, mission-critical WSN deployments such as IoT and industrial environments.

3. Proposed Methodology

3.1 Radio Model

This equation 1 represents the total energy consumption E_{Total} in a wireless sensor network, where is the energy used for transmission E_{TX}, energy required to receive the data (E_{RX}) which depends on the distance d and the number of bits l energy required for data aggregation E_{DA}

$$E_{Total} = E_{TX} + E_{RX} + E_{DA} \tag{1}$$

Equation 2 explain the energy consumption required for transmitting data E_{TX} in a wireless sensor network. It basically depends upon the number of bits and the distance d. Here is two conditions when $d < d_0$ and $d \geq d_0$ to compute the energy consumption required for transmitting data.

$$E_{tx}(l,d) = \begin{cases} l.E_{elec} + l.\varepsilon_{fs}d^2, d < d_0 \\ l.E_{elec} + l.\varepsilon_{fs}d^4, d \geq d_0 \end{cases} \tag{2}$$

Equation 3 represents the energy required to receive the data (E_{RX}) in a wireless sensor network. E_{RX} is directly proportional to the number of bits l received. The energy required to run the circuitry is denoted by E_{elec} . $l * E_{elec}$ denotes the total energy required to receive l bits of data.

$$E_{RX}(l) = l * E_{elec} \tag{3}$$

Equation 4 represents the energy required for data aggregation (E_{DA}) in a wireless sensor network. In the equation ε_{da} represents energy consumed per bit for data aggregation.

$$E_{DA}(l) = l * \varepsilon_{da} \tag{4}$$

Equation 5 shows the threshold distance in WSN. It is defined by the point where energy model of transmission has switches from free space to multi path fading.

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}. \tag{5}$$

When the transmitter and receiver is less then d_0 then free space model consider in energy consumption and multipath fading model adopted for energy consumption when d is greater than or equal to d_0.

3.2 *Polynomial Generation*

This equation defines a symmetric polynomial matrix P of degree t over a finite field F_q, where each element satisfies $\boldsymbol{a_{i,j}} = \boldsymbol{a_{j,i}}$. Such symmetry ensures consistent key generation for any pair of nodes, enabling secure and efficient communication in cryptographic systems.

$$P = \begin{bmatrix} a_{00} & a_{01} & \dots & a_{0t} \\ a_{10} & a_{11} & \dots & a_{1t} \\ \vdots & \vdots & \dots & \vdots \\ a_{t0} & a_{t1} & \dots & a_{tt} \end{bmatrix} \quad (6)$$

3.3 *Key Calculation*

The function to calculate the secure key $K_{i,j}$ between two nodes i and j uses a Homomorphic Polynomial Encryption-based approach to ensure robust encryption. The key $K_{i,j}$ is computed by evaluating a symmetric polynomial function at the IDs of the two nodes.

$$K_{i,j} = \sum_{m=0}^{t} \sum_{n=0}^{t} a_{m,n} \, X_i^m \, X_j^n \, mod \, q \quad (7)$$

3.4 *Integration with Adaptive Clustering*

After clustering the sensor nodes, the code assigns secure keys to each node based on its cluster head. Let B be the cluster assignment for each sensor nodes and A be the cluster head IDs. For the sensor node i with ID x_i and with its cluster head j x_j :

$$K_{i,j} = \sum_{m=0}^{t} \sum_{n=0}^{t} a_{m,n} \, X_i^m \, X_j^n \, mod \, q \quad (8)$$

This secure key $K_{i,j}$ is used for communication between the sensor node and its cluster head.

3.3Algorithm:

1. Polynomial Generation

```
function poly = generate polynomial (t, q)
poly = randi ([1 q-1], t+1, t+1);
poly = triu(poly) + triu (poly, 1)'; % Symmetric
end
```

Key Calculation

```
function key = polynomial_key (poly, xi, xj, q)
t = size (poly, 1) - 1;
key = 0;
for i = 0:t
for j = 0:t
key = mod (key + poly (i+1, j+1) * (xi^i) * (xj^j), q);
end
end
end
```

Integration with Clustering

```
t = 2; % Polynomial degree
q = 997; % Large prime modulus
poly = generate_polynomial (t, q);
```

```
node_ids = 1:scount; % Sensor IDs
secure_keys = zeros (1, scount);
for i = 1:scount
cluster_id = B(i);
ch_id = A(cluster_id);
xi = node_ids(i);
xj = node_ids(ch_id);
secure_keys(i) = polynomial_key(poly, xi, xj, q);
end
%
disp("Sensor-to-CH Secure Keys using Homomorphic Polynomial Encryption:");
for i = 1:scount
Display the secure keys
end
```

4. Results and Discussion

This study compares the proposed protocol to the LEACH, TEACH, and K-MEANS algorithms. Power consumption, the number of live nodes, and the throughput parameter has taken into consideration during the comparison research with the above algorithm to demonstrate the effectiveness of the suggested protocol. In this work, sensors are arranged in a clustered network architecture with a fixed size of four clusters, using a random normal distribution. For validating the result set of the experiment 64 sensors deployed in a 300 X 300 region in Netsim simulation tool and 5000 iterations has been performed to compute throughput and power consumption across all protocols.

4.1 *Analysis of Power Consumption:*

During the experiment we have found that LEACH and K Means consumptions are 50% greater than proposed algorithm, while TLEACH consumption is 55% more. So, during the study author found that proposed algorithm is the least power and most stable results shown by bar graph manner in figure 2.

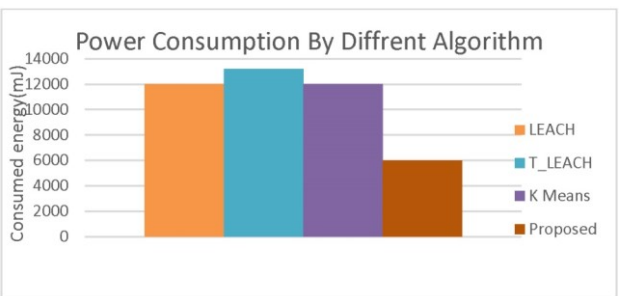

Figure 2
Power Consumption by Different Algorithm

4.2 *Analysis of throughput*

Throughput basically refers to the rate at successful data transfer between the sensor node to the base station. High throughput ensures efficient data transmission between the nodes which is crucial for many applications to collect data in an accurate time manner. Figure 3 shows the comparison of throughput of LEACH, T LEACH, K MEANS and proposed algorithm. In this analysis ANOVA test is implemented to find statistically significant differences between the algorithms. Results indicate that proposed algorithm 267.25% perform better than other algorithms close to 2.5 times better by other algorithms.

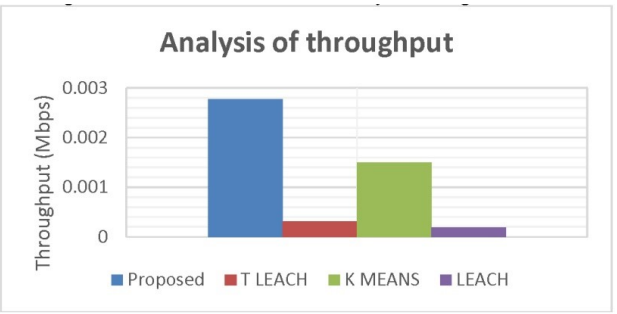

Figure 3
Analysis of throughput

4.3 *Analysis of Number of Alive nodes*

The summary of the analysis is that the LEACH algorithm performed well, keeping all the nodes alive until 2000 rounds. However, by 5000 rounds, it only kept 20% of the nodes alive. TLEACH did not start well from the beginning, with only 7.81% of nodes alive at 2000 rounds. K-MEANS had mixed performance, with 25% of nodes alive at 2000 rounds, peaking at 82.81% at 3000 rounds, but dropping to 26.67% by 5000 rounds. The proposed algorithms kept all the nodes alive up to 4000 rounds and slightly dropped to 93.75% at 5000 rounds comparison shown by figure 4.

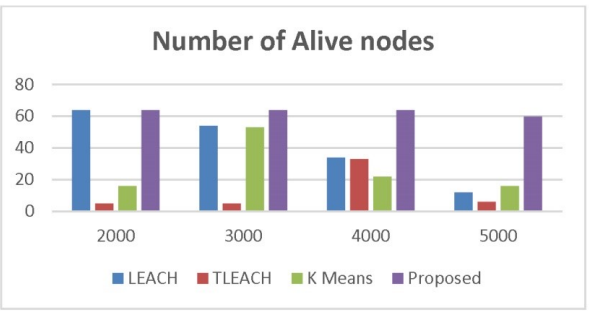

Figure 4
Number of Alive Nodes

Conclusion:

This research has proposed an optimized approach for enhancing the performance and security of Wireless Sensor Networks (WSNs) through adaptive clustering and homomorphic polynomial encryption technique. By leveraging Fuzzy C-Means clustering that considers both distance and residual energy, the protocol ensures efficient cluster head selection, thereby reducing energy consumption and prolonging network life. The integration of homomorphic polynomial encryption technique further ensures secure intra-cluster communication with minimal computational overhead. Simulation results confirm that the proposed method achieves a 52% reduction in power consumption, enhances throughput by 200.65%, and sustains a high number of alive nodes up to 5000 rounds. These results validate the proposed protocol's effectiveness in enhancing both the energy efficiency and security of WSNs, making it a viable and sustainable solution for real-world IoT and industry-driven sensor network applications.

References

[1] D. M. S. Bhatti, N. Saeed, and H. Nam, "Fuzzy C-means clustering and energy-efficient cluster head selection for cooperative sensor network," *Sensors*, vol. 16, no. 9, pp. 1461 (2016).

[2] P. S. Mehra, M. N. Doja, and B. Alam, "Fuzzy-based enhanced cluster head selection (FBECS) for WSN," *Procedia Computer Science,* vol. 132, pp. 1003–1010 (2018).

[3] R. Wan, N. Xiong, Q. Hu, H. Wang, and J. Shang, "Similarity-aware data aggregation using fuzzy C-means approach for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking,* vol. 2017, no. 1, pp. 1–17 (2017).

[4] A. R. Naderloo, S. A. F. Aghda, and M. Mirfakhraei, "Fuzzy-based cluster routing in wireless sensor networks," *Fuzzy Systems and Their Mathematics* (2023).

[5] D. Agrawal and S. Pandey, "Load-balanced fuzzy-based unequal clustering for wireless sensor networks assisted Internet of Things," *Engineering Reports*, vol. 2, no. 3, pp. e12130 (2020).

[6] R. P. S. Hada and A. Srivastava, "Dynamic cluster head selection in wireless sensor networks," *International Journal of Communication Systems,* vol. 35, no. 5, pp. e5037 (2022).

[7] R. Raj Priyadarshini and N. Sivakumar, "Cluster head selection based on minimum connected dominating set and bi-partite inspired

methodology for energy conservation in WSNs," *Procedia Computer Science*, vol. 125, pp. 160–167 (2018).

[8] S. Durugkar and R. C. Poonia, "Optimum utilization of natural resources for home garden using wireless sensor networks," *Journal of Information and Optimization Sciences*, vol. 38, no. 6, pp. 1077–1085 (2017).

[9] B. Das, S. Nandi, and S. Roy, "Dual-stage cluster formation using K-means and fuzzy logic in wireless sensor networks," *International Journal of Wireless and Mobile Computing*, vol. 17, no. 1, pp. 67–75 (2022).

[10] N. Chaudhary, S. Verma, and R. Gupta, "A multi-objective fuzzy-based cluster head selection algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 132, no. 1, pp. 91–112 (2023).

[11] M. D. Kokate, A. Julian, R. Ramyadevi, M. Rele, G. I. Mary, and M. Vaithianathan, "Enhancing network security in wireless sensor networks through real-time intrusion detection systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 5-A, pp. 1743–1751 (2025), doi: 10.47974/JDMSC-2174.

[12] S. Siddamsetti, M. M. Qasim, N. Sravanthi, K. Dinesh, V. Velmurugan, S. Sengan, and P. Dadheech, "Wireless sensor networks with modular metric spaces," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 2, pp. 659–667 (2025), doi: 10.47974/JIM-2109.

[13] D. Singh, N. Savarimuthu, D. Nagaraju, P. Vidyullatha, K. Maithili, M. Sasikumar, S. M. F. Ul-Haque, and M. Elangovan, "Energy-efficient wireless sensor networks for disaster management using hybrid technique," *Journal of Information and Optimization Sciences*, vol. 45, no. 8, pp. 2249–2259 (2024), doi: 10.47974/JIOS-1799.

[14] D. Goyal, A. Kumar, Y. Gandhi, and V. Khetani, "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 703–714 (2024), doi: 10.47974/JDMSC-1921.

Received May, 2025