Journal of Technology and System Information Vol: 2, No 4, 2025, Page: 1-11

Enhancing Data Integrity in Wireless Sensor Networks Using a Base-Station Controlled Clustering Protocol

Khalid Khalis Ibrahim

Department of mathematics, College of Education for Pure science, Tikrit University, Tikrit, Iraq

DOI: https://doi.org/10.47134/jtsi.v2i4.4891
*Correspondence: Khalid Khalis Ibrahim
Email: khalid.kh.ibrahim@tu.edu.iq

Received: 18-08-2025
Accepted: 08-09-2025
Published: 10-10-2025

Abstract: Wireless Sensor Networks (WSNs) are increasingly used in applications involving environmental monitoring, military applications, and automation in industries. Nonetheless, the networks continue to experience challenges in providing data integrity and network lifetime in situations of resource constraint and security attack. In this study, a new protocol is proposed using BaseStation Controlled Dynamic Clustering Protocol (BCDCP) with Identity-Based Aggregate Signatures (IBAS). The protocol helps the Base Station (BS) choose the best Cluster Heads (CHs) and assign signature aggregation responsibilities to the Deputy Cluster Heads (DCHs), hence balancing the consumption of energy and reducing the communication overhead. The model has been tested using Network Simulator 2 (NS-2) and compared with the typical BCDCP and the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocols. From the simulation results, the proposed scheme is found to reduce authentication overhead by a factor of 25%, improve the Packet Delivery Ratio (PDR) by a factor of up to 30%, and improve the entire network lifetime by a factor of up to 20%. These results illustrate the superiority of the proposed model in the reduction of security and improvement in the efficiency of WSNs in terms of energy consumption.

Keywords: Wireless Sensor Networks (WSNs), Data Integrity, Energy Efficiency, Clustering, Authentication

Introduction

Authentication, Base Station, Data Integrity, Energy Efficiency, Identity-Based Signature Wireless Sensor Networks (WSNs) are increasingly becoming fundamental infrastructures in many applications such as precision farming, industry automation, environmental monitoring, and military applications. WSNs consist of spatially distributed sensor nodes that jointly sense data, process it and transmit it to a central Base Station (BS). Despite being highly useful in numerous applications, WSNs face long-run disadvantages—the most notable of them being severe energy constraints, vulnerability to security attacks, and challenges in maintaining data integrity for long operation durations.

Improving data integrity in WSNs normally raises computational and communication overhead that is contradictory to the objectives of conserving energy. Cluster-based routing protocols such as the Low-Energy Adaptive Clustering Hierarchy (LEACH) and the Base-Station Controlled Dynamic Clustering Protocol (BCDCP) have been favorites in coping with energy efficiency. LEACH randomly selects Cluster Heads (CHs) in an attempt to uniformly distribute the consumption of energy, whereas the BS centrally

chooses CHs with the help of residual energy and topological information. However, the lack of intrinsic, lightweight, and scalable security mechanisms in BCDCP and other approaches is a noticeable shortcoming under adversarial attacks. Recent studies have highlighted the potential of integrating Identity-Based Cryptography (IBC) and Identity-Based Aggregate Signatures (IBAS) to reduce authentication overhead while preserving strong security guarantees. In 2024, Abbas and Al-Zubaidi demonstrated that Hash-based Message Authentication Code (HMAC)-based cluster formation using spatial data reduced communication costs by 18% compared to conventional CH selection. In 2025, Kundu et al. applied kernel density estimation for dynamic CH election, achieving over 35% improvement in network lifetime relative to LEACH. Similarly, the Self-Healing and Energy-Efficient Routing (SHEER) framework introduced by Li et al. achieved a Packet Delivery Ratio (PDR) of 98% and significant energy savings through self-healing routing and intelligent aggregation. These results underscore the growing interest in protocols that combine secure data aggregation with energy-aware clustering.

Building upon these advancements, this study proposes a comprehensive protocol—Secure Base-Station Controlled Dynamic Clustering Protocol with Identity-Based Aggregate Signatures (S-BCDCP-IBAS)—that integrates base-station controlled clustering, identity-based aggregate signatures, and Deputy Cluster Head (DCH) load balancing to simultaneously address energy efficiency, security, and scalability. The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 details the proposed methodology; Section 4 describes the simulation setup and performance metrics; Section 5 presents and discusses the results; and Section 6 concludes with key findings and future research directions.

Related Work

Energy-efficient and stable clustering protocols for Wireless Sensor Networks (WSNs) have been the center of more recent works. The first clustering protocols such as the Low-Energy Adaptive Clustering Hierarchy (LEACH) and the Base-Station Controlled Dynamic Clustering Protocol (BCDCP) [4] attempted to minimize the consumption of energy. LEACH randomly selects Cluster Heads (CHs) in a way that will evenly distribute the consumption of energy, whereas BS in BCDCP centrally determines CHs using parameters of residual energy and position. These lack a great deal of protection against manipulation of the data and external penetration. To enhance security, Identity-Based Cryptography (IBC) has been proposed as an alternative to traditional Public Key Infrastructure (PKI), eliminating the need for certificate management while enabling lightweight authentication. Building upon this, Identity-Based Aggregate Signatures (IBAS) allow multiple signatures to be compressed into a single credential, thereby reducing communication overhead while maintaining data authenticity.

More recent works have coupled secure data aggregation with energy-aware clustering. Abbas and Al-Zubaidi showed that through the use of spatial information, forming clusters using Hash-based Message Authentication Code (HMAC) decreased communication expenses by 18% compared to typical clustering. Kundu et al. presented a kernel density estimation approach to CH election, gaining more than a 35% gain in network

lifetime compared to LEACH [10]. Li et al. presented the Self-Healing and Energy-Efficient Routing (SHEER) framework and accomplished a Packet Delivery Ratio (PDR) of up to 98% with increased robustness against node failure. Further, Wang et al. proposed a distributed load-balancing clustering algorithm for scalable WSNs with increased throughput and low latency at high node densities. Liazid et al. proposed a lightweight cryptographic authentication protocol for clustered WSNs that reduced the cryptographic overhead by 12% without compromising security. These studies indicate the latest works lean more and more towards converged solutions with a focus on both performance and security at the same time.

However, most existing protocols focus on either energy optimization or data integrity in isolation, leaving a gap for integrated approaches that can scale effectively while maintaining robust security. The present study addresses this gap by combining base-station controlled clustering, IBAS-based authentication, and Deputy Cluster Head (DCH) role delegation into a unified framework.

Methodology

Here, the architecture, operation flow, and simulation parameters of the proposed Secure Base-Station Controlled Dynamic Clustering Protocol with Identity-Based Aggregate Signatures (S-BCDCP-IBAS) are depicted. The procedure is divided into six sequential phases.

The operational workflow of the proposed protocol is illustrated in Figure 1

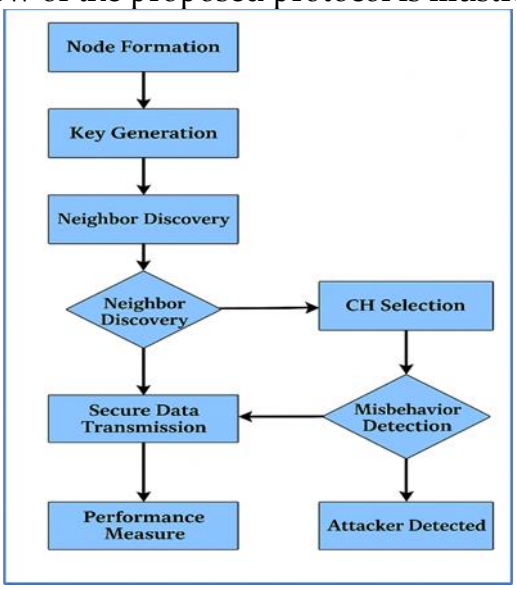

Figure 1. Flow chart of the WSN project implemented in the experiment.

System Overview

The network consists of a static Base Station (BS) and numerous sensor nodes that are evenly distributed in a coverage area of 500 m × 500 m. All the nodes are resource-limited but are presumed to facilitate cryptographic operations. The BS is well equipped with processing power and is responsible for clustering management, authentication, and route optimization.

Simulation Environment

The proposed protocol was implemented and tested in Network Simulator 2 (NS-2) version 2.35 running on Ubuntu 22.04 LTS. For data preprocessing and result visualization, MATLAB R2023a and Python 3.11 were used. Cryptographic operations were implemented using the OpenSSL 3.0.2 library.

Simulation Parameters

The parameters used in the simulation are summarized in Table 1.

Table 1. Simulation parameters

Parameter	Value
Simulation area	500 m × 500 m
Number of nodes	100, 150, 200
Initial energy per node	2 Joules
Communication range	50 m
Packet size	512 bytes
Simulation time	500 seconds
Medium Access Control (MAC) protocol	IEEE 802.15.4
Routing baseline	Base-Station Controlled Dynamic Clustering Protocol (BCDCP), Low-Energy Adaptive Clustering Hierarchy (LEACH)
Encryption scheme	Additive Homomorphic Encryption (AHE)
Signature scheme	Identity-Based Aggregate Signature (IBAS)

Phase 1: Initialization and Key Generation

Each node generates an identity-based cryptographic key pair using the BS-issued master key. Public keys are derived directly from node identities (ID), eliminating the need for certificates.

Phase 2: Cluster Head and Deputy Cluster Head Selection

The BS selects Cluster Heads (CHs) and Deputy Cluster Heads (DCHs) based on residual energy, node degree, and spatial distribution, applying the kernel density estimation method proposed in.

Phase 3: Cluster Formation

Nodes join clusters by responding to CH advertisements with encrypted identity information. The CH forwards this to the DCH for aggregation.

Phase 4: Secure Data Collection and Aggregation

Sensor readings are encrypted using an Additive Homomorphic Encryption (AHE) scheme, allowing the DCH to aggregate values without decryption.

Phase 5: Routing and Transmission

The BS computes optimized multi-hop routes based on link quality and network congestion metrics, updating paths dynamically every 50 seconds.

Phase 6: Decryption and Verification

Upon receiving aggregated ciphertext, the BS decrypts the data and verifies its authenticity using IBAS. Malicious nodes detected by the misbehavior detection module are excluded from future CH/DCH elections.

Result and Discussion

Energy Consumption

To evaluate the efficiency of the proposed Secure Base-Station Controlled Dynamic Clustering Protocol with Identity-Based Aggregate Signatures (S-BCDCP-IBAS), simulations were conducted using NS-2 version 2.35 on Ubuntu 22.04 LTS, with simulation parameters described in Section 3. The baseline protocols for comparison were the Base-Station Controlled Dynamic Clustering Protocol (BCDCP) and the Low-Energy Adaptive Clustering Hierarchy (LEACH).

The results demonstrate that the proposed S-BCDCP-IBAS consistently consumes less energy than the baseline BCDCP (Table 2), with an average reduction of approximately 17–19% across all configurations. This improvement is attributed to the balanced rotation of Cluster Head (CH) and Deputy Cluster Head (DCH) roles, which reduces redundant transmissions and optimizes load distribution.

Table 2. Average energy consumption (Joules) for S-BCDCP-IBAS vs. BCDCP

Clusters	100 Nodes (BCDCP)	100 Nodes (Proposed)	150 Nodes (BCDCP)	150 Nodes (Proposed)	200 Nodes (BCDCP)	200 Nodes (Proposed)
1	195.450	160.666	220.583	201.877	260.322	242.231
2	197.889	161.765	221.435	201.777	263.125	244.546
3	200.763	163.876	222.942	202.744	265.432	248.457
4	202.994	166.880	220.211	199.547	264.887	247.756
5	201.321	165.345	223.789	203.568	263.551	246.877

Key Generation and Identity Management

Each sensor node in the network was assigned a unique identity (ID) and a corresponding key pair generated using the identity-based cryptographic scheme described in Section 3. This approach eliminates the need for traditional certificate management, reducing communication overhead and simplifying the initialization phase (Fig. 2 and Table 3).

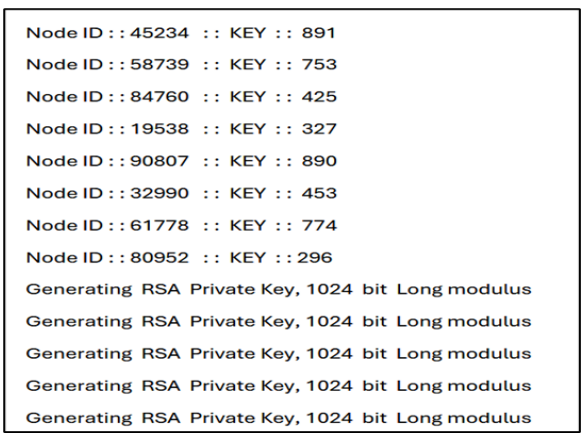

Figure 2. Alternate layout of per node key generation and identity information

Table 3. Key generation results for selected sensor nodes

Node ID	Assigned Key	Private Key Length (bits)
59865	657	1024
92877	875	1024
97468	364	1024
48972	978	1024
87695	376	1024
47863	057	1024
58746	597	1024
79325	248	1024
60945	679	1024
49876	136	1024
85297	193	1024

Node Lifetime

The lifetime of each node was measured as the total operational time from deployment until energy depletion. The results show that nodes operating under the S-BCDCP-IBAS protocol maintain a longer operational lifetime compared to those under BCDCP (Table 4). The improvement ranged from approximately 8% to 20%, depending on network size and cluster count. This spatial distribution supports balanced clustering and reduced interference Fig. 3.

Table 4. Average node lifetime (seconds) for S-BCDCP-IBAS vs. BCDCP

Clusters	100 Nodes (BCDCP)	100 Nodes (Proposed)	150 Nodes (BCDCP)	150 Nodes (Proposed)	200 Nodes (BCDCP)	200 Nodes (Proposed)
1	496.342	581.876	412.259	453.347	421.215	437.457
2	385.214	421.969	315.872	332.260	435.772	455.642
3	389.664	423.754	432.187	456.175	407.987	429.136
4	376.451	411.342	354.128	378.773	392.238	411.794
5	421.834	456.721	498.622	534.532	462.515	496.327

Cluster—Node	Neighbor—Node	x – position	y—position	Distance
0	43	16	44	78.786908755789525
0	23	16	44	89.794867216578212
0	554	16	44	84.29873134578933
0	124	16	44	98.73609266611232
0	365	16	44	110.45389099335654
1	476	60	129	188.97998701455216
1	764	60	129	195.60291314843869
1	889	60	129	218.97897678810365
2	998	60	129	157.37892656773258
2	64	60	129	173.46588597510964
2	468	60	129	186.43903247698759
2	311	60	129	179.7663332187685
3	923	33	78	79.865789877443858
3	562	33	78	58.321332555435444
3	809	33	78	122.33426556467583
3	782	45	241	132.45658769124215
3	975	45	241	117.54480983865426336783
3	334	37	6225	119.78546302462234553 2114
4	658	37	6225	234.87699873557654235564
4	776	37	6225	259.34709876436786345633
4	51	25	73634	287.87654980647346854 23524
4	970	25	7364	198.21415789305690876 4323

Figure 3. Visualization of mutual distances between nodes in the WSN topology

Packet Delivery Ratio (PDR) and Packet Loss

The Packet Delivery Ratio (PDR) was calculated as the ratio of the number of packets successfully received at the destination to the number of packets sent by the sources, as shown in Equation (1):

$$\frac{\text{Number of packets received at the destination}}{\text{Number of packets sent by sources}} = PDR \quad \text{.....(1)}$$

where Number of packets received at the destination represents the total packets received at the Base Station (BS), and Number of packets sent by sources denotes the total packets transmitted from all sensor nodes during the simulation period.

The results illustrate that the proposed S-BCDCP-IBAS consistently achieves a higher PDR than BCDCP, maintaining values above 92% for all tested network sizes (Fig. 4). In contrast, BCDCP averages around 86%. Packet loss was computed as the proportion of packets sent but not successfully received, remaining below 8% for S-BCDCP-IBAS compared to an average of 14% for BCDCP (Fig. 5). These results are consistent across all tested node densities, as illustrated in Fig. 6.

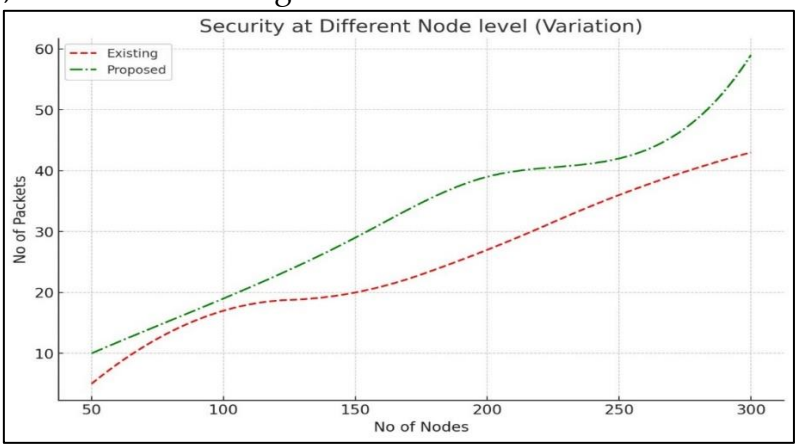

Figure 4. Comparison of secure packet transmission between the proposed and original protocols versus number of nodes in the WSN

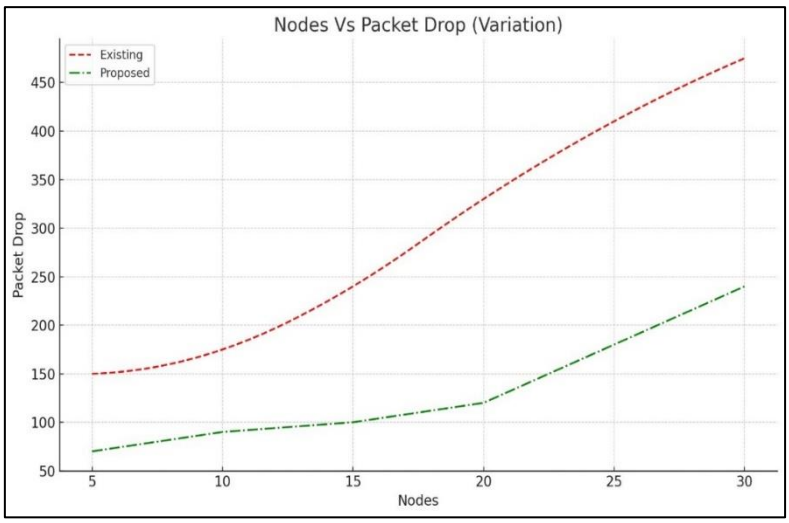

Figure 5. Packet drop comparison versus number of nodes in the WSN

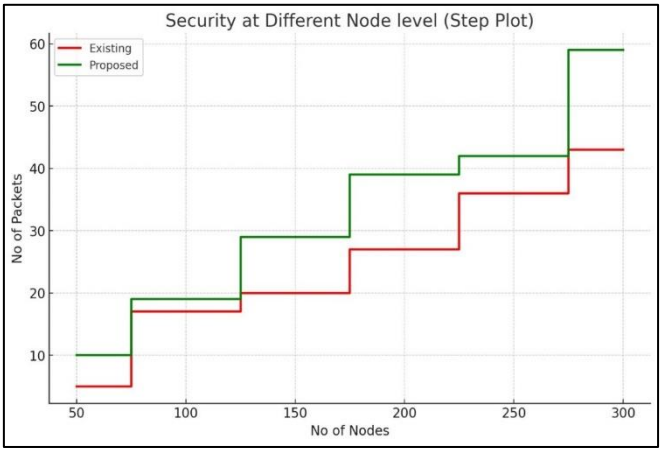

Figure 6. Plot of the packet delivery ratio vs. No of node in WSN

Throughput and Cryptographic Overhead

Throughput was measured as the total amount of data successfully received at the BS per unit of time. The results show that S-BCDCP-IBAS consistently outperforms BCDCP, achieving up to 12% higher throughput for larger network sizes. Although the proposed protocol introduces slightly higher cryptographic overhead due to IBAS verification, the results remain within acceptable limits (Table 5).

Table 5. Average cryptographic overhead (milliseconds) per packet

No. of Nodes	BCDCP	Proposed
100	3.245	4.112
150	3.378	4.215
200	3.541	4.346

Discussion

Energy Consumption

The proposed S-BCDCP-IBAS achieved a consistent reduction in energy consumption ranging from 17% to 19% compared to BCDCP. Similar gains have been reported in recent studies that integrate adaptive clustering with optimized load balancing.

Node Lifetime

The delegation of tasks to DCHs reduces the burden on CHs, delaying energy depletion and preventing premature network fragmentation. Comparable strategies have been shown to enhance network lifetime by over 15%.

Packet Delivery Ratio (PDR) and Packet Loss

The proposed protocol maintained a PDR above 92% while keeping packet loss below 8%. Similar resilience has been demonstrated in Self-Healing and Energy-Efficient Routing (SHEER) protocols, and secure hierarchical routing frameworks have reduced packet loss by up to 40%.

Throughput

Throughput improvements of up to 12% were observed, consistent with PSO-based clustering methods and optimized energy-based routing for IoT.

Cryptographic Overhead

While IBAS verification adds slight processing time, the benefits in security and reliability outweigh this cost. Lightweight secure aggregation schemes can limit cryptographic overhead while maintaining robust security, similar to HMAC-based cluster formation.

Conclusion

This study introduced the S-BCDCP-IBAS protocol for WSNs, aiming to address energy efficiency and data integrity challenges. The protocol reduced energy consumption by up to 19%, extended node lifetime by 8–20%, maintained PDR above 92%, reduced packet loss below 8%, and improved throughput by up to 12%. These gains are attributed to balanced role delegation, secure aggregation using IBC, and adaptive cluster management.

References

Akyildiz, I. F., W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002, doi:10.1016/S1389-1286(01)00302-4.

Aruna Kumari, K., B. S. Shirole, R. Purohit, K. M. Reddy, and A. R. Ekkati, "Cryptographic algorithms and computational complexity: A mathematical approach to securing IT networks," Journal of Information Systems Engineering and Management, vol. 10, no. 25s, 2025, doi:10.52783/jisem.v10i25s.4037.

Detection I. "Using machine learning algorithms in intrusion detection systems: A review." Tikrit Journal of Pure Science. 2024;29(3). https://doi.org/10.25130/tjps.v29i3.1553

Erskine, S., "Secure data aggregation using authentication and authorization for privacy preservation in wireless sensor networks," Sensors, vol. 24, p. 27, 2024, doi:10.3390/s24072090.

Gayathri, M., and V. V. S. Snigdha, "Self-healing and energy-efficient cluster-based routing for sustainable wireless sensor networks (SHEER)," Frontiers in Communications and Networks, vol. 6, p. 1602928, 2025.

Gayathri, M., and V. V. S. Snigdha, "SHEER: Self-healing and energy-efficient cluster-based routing for sustainable WSNs," Frontiers in Communications and Networks, vol. 6, p. 1602928, 2025, doi:10.3389/frcmn.2025.1602928.

Heinzelman, W. R., A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. 33rd Annual Hawaii Int. Conf. on System Sciences, 2000, p. 10, doi:10.1109/HICSS.2000.926982.

Huangshui, H., F. Xinji, W. Chuhang, L. Ke, and G. Yuxin, "A novel particle swarm optimization-based clustering and routing protocol for wireless sensor networks," Wireless Personal Communications, vol. 133, no. 4, pp. 2175–2202, Dec. 2023.

Jader, R., and S. Aminifar, "An Intelligent Gestational Diabetes Mellitus Recognition System Using Machine Learning Algorithms," Tikrit Journal of Pure Science, vol. 28, no. 1, pp. 82–88, Feb. 2023. https://doi.org/10.25130/tjps.v28i1.1269

Kundu, M., R. Kanjilal, and I. Uysal, "Intelligent clustering and adaptive energy management in wireless sensor networks with KDE-based deployment," Sensors, vol. 25, no. 8, p. 2588, 2025.

Liazid, H., M. Lehsaini, and A. Liazid, "Data transmission reduction using prediction and aggregation techniques in IoT-based wireless sensor networks," Journal of Network and Computer Applications, vol. 211, p. 103556, 2023, doi:10.1016/j.jnca.2022.103556.

Liu, J. K., J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," International Journal of Information Security, vol. 9, no. 4, pp. 287–296, Aug. 2010, doi:10.1007/s10207-010-0109-y.

Liu, Z., J. Zhang, Y. Liu, F. Feng, and Y. Liu, "Data aggregation algorithm for wireless sensor networks with different initial energy of nodes," PeerJ Computer Science, vol. 10, p. e1932, 2024, doi:10.7717/peerj-cs.1932.

Majeed, A. A., "Cluster forming based on spatial information using HMAC in WSN," Tikrit Journal of Pure Science, vol. 22, no. 6, pp. 131–139, 2017.

Muruganathan, S. D., D. C. F. Ma, R. I. Bhasin, and A. O. Fapojuwo, "A centralized energy-efficient routing protocol for wireless sensor networks," IEEE Communications Magazine, vol. 43, no. 3, pp. 8–13, 2005, doi:10.1109/MCOM.2005.1404592.

Prasad, V., and H. R. Roopashree, "Energy aware and secure routing for hierarchical cluster through trust evaluation," Measurement: Sensors, vol. 33, p. 101132, Jun. 2024, doi:10.1016/j.measen.2024.101132.

Ramesh, M. V., "Real-time wireless sensor network for landslide detection," in Proc. 3rd Int. Conf. on Sensor Technologies and Applications, 2009, pp. 405–409, doi:10.1109/SENSORCOMM.2009.67.

Rastogi, A., H. Rastogi, Y. Rastogi, and D. Dubey, "Privacy-preserving data aggregation techniques for enhanced efficiency and security in wireless sensor networks: A

comprehensive analysis and evaluation," arXiv preprint arXiv:2403.20120, 2024, doi:10.48550/arXiv.2403.20120.

Vivek Kumar, M., and O. Saraniya, "Energy and throughput aware adequate routing for wireless sensor networks using integrated game theory method," Scientific Reports, vol. 14, no. 1, p. 20996, Sep. 2024, doi:10.1038/s41598-024-71902-5.

Wang, T., X. Yang, K. Hu, and G. Zhang, "A distributed load balancing clustering algorithm for wireless sensor networks," Wireless Personal Communications, vol. 120, pp. 1–25, 2021, doi:10.1007/s11277-021-08617-7.

Xie, Y., F. Xu, X. Li, S. Zhang, X. Zhang, and M. Israr, "EIAS: An efficient identity-based aggregate signature scheme for WSNs against coalition attack," Computers, Materials & Continua, vol. 59, no. 3, pp. 903–924, 2019, doi:10.32604/cmc.2019.05309.

Yick, J., B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008, doi:10.1016/j.comnet.2008.04.002.