SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

A Reliable, Energy-Efficient And Secure Data Aggregation Framework For Resource-Constrained Wireless Sensor Networks

Bansude Vijaysinh Uttamrao[1] , Dr. Rahul Kumar Budania[2] , Dr. Shrinivas Tanaji Shirkande[3] , Zade Mahesh Mahadev[4]

[1]Research Scholar at Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan & Assistant Professor at S B Patil College of Engineering, Indapur(Maharashtra) Vijubansude@gmail.com
[2]Associate Professor at Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan rahulbudania93@gmail.com
[3]Associate Professor at S B Patil College of Engineering, Indapur(Maharashtra) shri.shirkande8@gmail.com
[4]Research Scholar at Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan & Assistant Professor at S K N Sinhgad College of Engineering, Korti,Pandharpur(Maharashtra) zademahesh1983@gmail.com

Abstract
Wireless Sensor Networks (WSNs) are ubiquitous to continuous sensing and remote monitoring applications, where a multitude of resource-limited sensor nodes collect and send environmental data to a base station. With so many sensor nodes placed in close proximity to each other, the collected data may have high spatial and temporal correlation that can lead to unnecessary data transmission, high energy consumption, packet collisions, communication delay, and short network lifetime. While current aggregation schemes often tackle energy saving, data reliability, scheduling, and security as separate issues, data aggregation is a good way to reduce unwanted transmissions. This makes it unsuitable to use in resource constrained WSNs, where these requirements are tightly coupled. In this paper, we propose a framework named Adaptive Reliability-Aware Secure Data Aggregation (ARSDA) which incorporates data filtering, reliability assessment, energy-aware forwarding, as well as secure aggregation. First, abnormal observations in the sensors are detected by the Exponential Moving Average (EMA) with adaptive threshold, which also filters out redundant observations. The sensor observations are then aggregated based on similarity. Based on the residual energy, data reliability, similarity quality and transmission distance, a reliability-energy score is used to select the appropriate forwarding nodes. To maintain the confidentiality and integrity of the information transmitted, while keeping security related overhead to a minimum, secure aggregation is provided. Evaluation using network, aggregation, reliability, and security measures for simulation based on ARSDA, LEACH, and RSDA. The proposed ARSDA shows 98.2% data accuracy, 1780 round of network lifetime, 1.9% packet loss ratio and 98.1% packet delivery ratio. Results show that a combination of reliability-aware aggregation with energy-aware forwarding and light-weight security scheme is actually feasible for prolonging the WSN life with reliable and secure data delivery.

Keywords: Wireless Sensor Networks, Data Aggregation, Energy Efficiency, Data Reliability, Secure Aggregation, Network Lifetime.

• Introduction

A Wireless Sensor Network (WSN) is a collection of spatially-distributed sensor nodes which monitor physical or environmental conditions and send the sensed data to a sink or base station. They have been deployed in environmental monitoring, healthcare, agriculture, industrial monitoring etc. due to their relatively simple deployment and autonomous sensing capabilities. Typically a sensor node is able to sense, process locally, and wirelessly transmit with limited amount of power. Therefore, how the sensed information is processed and sent affects network's lifetime [1].

Battery power is of great concern since sensor nodes are often battery-powered and deployed in places where changing batteries or recharging them is challenging. A significant amount of node energy is spent on communication, especially if the raw observations are transmitted multiple times via multiple hops. This is exacerbated by dense deployment of sensors, where adjacent sensors often see the same physical phenomenon. Consequently, large amounts of information, in space and time, may be sent to the base station, but only a small portion of the information is useful in terms of new information [2]. The presented study also finds that repetitive sensing and transmission are causing network bottlenecks and early drain of the limited resources in WSNs.
To solve this problem, data aggregation is used to process the data within the network and only send the representative data, not all the data readings. Some intermediate nodes or cluster heads may aggregate observations from several sensor nodes, for example by averaging, adding, taking the minimum or maximum of the observations, or by performing similarity-based operations. With fewer and smaller packets to transmit, communication traffic can be reduced and energy saved. But too much aggregation can cause the loss of meaningful observations and consequently make the data reported to the base station less reliable [3]. Thus, it is crucial to have a proper balance between redundancy reduction and useful sensor information preservation for an effective aggregation scheme.
Aggregation performance is also impacted by network communication. Simultaneous transmissions, interference, packet collisions, retransmissions and extra energy expenditure can occur due to poor scheduling. The WRDAS approach studied in the foundational work solves this problem by using node ranking according to residual energy, sink distance, and neighborhood information, and then using TDMA-based scheduling with the information of two-hop neighborhood. The results reported show that a proper scheduling can significantly decrease the number of conflict packets and contribute to prolonging network lifetime.
Security is a consideration, too. Aggregator nodes are attractive targets for attack because they aggregate information from multiple sensors. Transmissions could be intercepted, sensor readings could be manipulated, false information could be introduced, or intermediate nodes could be compromised by an adversary. Intermediate nodes may need to decrypt information before aggregation, which means that the sensed information will be exposed in conventional hop-by-hop security [4]. This weakness can be mitigated by end-to-end secure aggregation, but this comes at a cost of more computation, communication and energy consumption. The basic conflict identified by the underlying study is thus between the reduction of communication achieved by aggregation, and the overhead of security mechanisms.

• Limitation In Existing Work

There are several data aggregation approaches in the field of WSNs, but most of them focus on one way to solve the problem. The main idea of energy-oriented protocols is to reduce the transmission frequency or to keep the energy in the nodes balanced. Scheduling methods target collision and latency minimization, and secure aggregation protocols target confidentiality and integrity. Reliability mechanisms, on the other hand, aim to recognize false, abnormal or contradictory sensor data. Considering these functions separately can lead to undesirable compromises. For instance, excessive redundancy filtering can reduce the cost of communication but still remove significant observations; the cryptographic processes can give greater security but be more energy intensive [5].
One disadvantage is the use of static thresholds to define the redundancy or abnormality of sensed observations. The measurement of a sensor is subject to natural variation with ambient conditions. A fixed threshold will thus incorrectly flag valid changes as anomalies or leave unwanted readings in when network conditions are altered. Likewise, forwarding is done solely according to the remaining energy and not whether a node will provide reliable information [6]. This might mean that a node with high residual energy but bad data reliability may be given high forwarding priority.
In view of these problems, this study proposes Adaptive Reliability-Aware Secure Data Aggregation (ARSDA) framework. ARSDA integrates all the above techniques: adaptive data filtering, similarity-based aggregation, reliability assessment, energy-aware forwarding, and secure communication in a single processing sequence. The method builds upon the previously mentioned paper, where Exponential Moving Average (EMA), threshold-based outlier detection and distance-based aggregation are used to cope with temporal and spatial redundancies. The following two research objectives are followed:

- Objective 1: Design an adaptive and reliability-aware data aggregation mechanism to minimize the redundant and abnormal data transmission of the sensors, maintain accuracy of the aggregated information, and save the energy of the sensor-nodes.
- Objective 2: Construct an energy-aware and secure forwarding mechanism that is based on residual energy, node reliability and considering the similarity of data and distance of transmission and maintaining the confidentiality and integrity of aggregated sensor information.

Raw sensor readings are first analyzed in ARSDA using EMA that allows capturing recent sensing behavior without keeping a large history of observations. A threshold is then applied to determine if the observation is significant or redundant or abnormal. Valid readings of a similar type are aggregated prior to transmission. However, ARSDA assigns a reliability-energy score to each node considering energy, reliability, similarity quality and distance. Nodes having appropriate scores are given forwarding priority and this will reduce the use of weak or unreliable nodes.

Security is added after local data reduction is done, which means that cryptographic processing is done on a smaller amount of information. This ordering is designed to regulate the security relevant communication and computation costs. The general idea is to secure aggregation as stated in the underlying research, and use EC-ElGamal based aggregation and integrity protection to maintain information when being sent.

• Proposed Direction And Paper Contribution

The primary value-add of ARSDA is that it treats reliability, energy consumption, redundancy reduction, forwarding and security not as unrelated network functions. The first process of observations made by sensors is adaptive filtering and elimination of redundancy. Then, reliable information is grouped based on similarity, and forwarding nodes based on the overall reliability-energy criterion are selected. Lastly, data is aggregated before multi-hopping to the base station.

The proposed framework is evaluated based on LEACH, WRDAS and RSDA with the following parameters: energy consumption, end-to-end delay, packet delivery ratio, network lifetime, aggregation ratio, redundancy reduction, data accuracy, packet loss, communication overhead, and data integrity. According to the proposed simulation results, ARSDA achieves 98.1% packet delivery ratio, 98.2% data accuracy and 1780 rounds network lifetime. These show that it is possible to reduce the amount of unnecessary information transmitted before it is securely sent, to reduce the amount of traffic on the network, and that reliability-aware forwarding can reduce the amount of nodes dependent on weak or inconsistent nodes.

The rest of this paper discusses the related WSN aggregation approaches, the ARSDA system model and methodology, the simulation environment and evaluation measures, the comparative results and finally the limitations and directions for the further investigation.

• Literature Review

Wireless Sensor Networks depend on data aggregation to reduce redundant transmissions, conserve limited node energy, and support dependable information delivery. Recent studies have examined energy-aware aggregation, prediction-based redundancy reduction, dual-layer aggregation, privacy preservation, and secure data transmission.

Table Analysis of existing works

Author	Main Approach	Key Parameters / Focus	Major Contribution	Limitation / Research Gap
Sheena et al. [7]	Energy-conscious data aggregation	Energy, PDR, lifetime, overhead	Reduced energy consumption during WSN data aggregation	Security and reliability-aware aggregation require further consideration
Yang et al. [8]	Dual-layer clustered aggregation	Data reduction, energy, clustering, transmission	Two-level aggregation reduces redundant communication	Limited consideration of secure and reliability-aware forwarding
Jain et al. [9]	Blockchain and ML-based secure	Security, trust, aggregation, attack detection	Combines security mechanisms with learning-based	Blockchain and ML can increase computation and resource requirements

	aggregation		aggregation	
Jain et al. [10]	Two-vector data prediction	Prediction, redundancy, energy, transmission	Reduces unnecessary sensor transmissions through data prediction	Primarily concerned with energy and prediction rather than end-to-end security
Liu et al. [11]	Energy-aware data aggregation	Residual energy, node lifetime, aggregation	Handles nodes having different initial energy levels	Reliability and security are not the primary aggregation criteria
Zhang et al. [12]	Privacy and integrity-preserving aggregation	Privacy, integrity, communication cost, aggregation	Protects aggregated sensor information and its integrity	Security mechanisms introduce additional processing and communication requirements
Heidari et al. [13]	Hybrid optimization and density correlation	Reliability, correlation, aggregation, optimization	Improves reliable aggregation using correlation and optimization	Higher algorithmic complexity may affect resource-constrained nodes
Begum et al. [14]	Comparative aggregation study	Energy, latency, reliability, security, aggregation	Identifies major requirements and limitations of WSN/IoT aggregation methods	Existing approaches struggle to jointly address multiple aggregation requirements

However, most existing methods address energy consumption, reliability, redundancy, forwarding, or security independently. Prediction and aggregation methods may lack security, while security-oriented schemes can introduce additional computational and communication overhead. Reliability of individual sensor observations is also not consistently considered during forwarding decisions. To address these limitations, the proposed ARSDA framework combines EMA-based adaptive filtering, reliability assessment, similarity-based aggregation, energy-aware forwarding, TDMA scheduling, and secure aggregation within a unified processing sequence. Thus, ARSDA aims to balance data reliability, energy conservation, communication performance, and security while extending the operational lifetime of resource-constrained WSNs.

• Proposed Methodology

This study aims to propose Adaptive Reliability-Aware Secure Data Aggregation (ARSDA) framework to reduce redundant transmissions, conserve sensor-node energy, maintain data reliability and secure aggregated data in the resource-constrained Wireless Sensor Networks (WSNs). The framework is based on the static multi-hop network configuration adopted in the work that is considered as underlying information, in which the information processed in the sensor nodes is forwarded to a fixed base station (BS) via a chain of aggregation nodes. The source, aggregator, and BS nodes are used in the tree-type network model in the original work. To this end, ARSDA implements adaptive filtering, reliability assessment, energy-aware forwarding, and secure aggregation.

• Simulation setup

The proposed ARSDA framework is analyzed by means of a simulation-based experiment using OMNeT++ as this is the simulation environment adopted in the underlying study detail shown in table-1. The sensor network is placed in a 500×500 m^2 area with a fixed base station located at the upper-middle part of the sensing area. To observe the behavior of ARSDA for different sizes of networks, the number of sensor nodes is varied between 100 to 500. The initial value of energy in each sensor node is set to 100 J and the uniform communication range of each sensor node is set to 60 m. Topology in the network does not change in each simulation. For performance measurement, it is assumed that the simulation runs for 500 s. Each experimental configuration is repeated 30 times in the original study, and the results averaged; the same is done with ARSDA, to minimize the effect of the random placement of nodes on the measured results. Energy, communication, aggregation, reliability and security are taken as measures to compare ARSDA with LEACH, WRDAS and RSDA.

Table Simulation Parameters for ARSDA

Parameter	Simulation Value
Network Simulator	OMNeT++
Deployment Area	500 × 500 m^2
Number of Sensor Nodes	100–500
Base Station	1, fixed
Network Topology	Static
Communication Radius	60 m
Initial Node Energy	100 J
Simulation Duration / Runs	• / 30 runs

• Network and Energy Model

Let us assume a WSN composed of n stationary sensor nodes, which are randomly placed in a 500 × 500 m^2 sensing field. The initial energy of each node is 100 J and the transmission range is 60 m, as set in the simulation of the underlying study. The distance between sensor and a candidate forwarding node shown in eq.1:

(1)

In this case, is the Euclidean distance of communication between $_i$ are the coordinates of source node are the coordinates of forwarding node . Distance is taken into account since more energy is needed to transmit over longer communication line.

The communication energy for a packet of L bits is modelled with a first order radio model shown in eq.2:

(2)

where is the energy consumed in the transmission, L is the length of the packet in bits, is the electronic energy of the circuits per bit, is the coefficient of the transmitter amplifier and d_{ij} is the distance of the transmission. In the next step, this energy term is taken into account in choosing the forwarding node.

• Adaptive Sensor Data Filtering

Often sensor nodes are placed in the vicinity of each other, rendering their measurements to be temporally correlated. The first step ARSDA takes is to obtain a light reference of the current sensing behaviour by applying an Exponential Moving Average (EMA) as shown in eq.3:

(3)

where is the smoothed value of the sensor is the current sensed value, is the previous smoothed value and λ is a smoothing coefficient in the range . The research conducted also employs EMA and threshold-based outlier processing for node-level aggregation. Rather than just a set threshold, ARSDA identifies if the current observation is very different from its recent behavior represent in eq.4:

(4)

where is the deviation of the current observation, is the sensed observation reading and is the smoothed reference value of the observation. If a reading is significantly different, it is flagged for reliability and not added to aggregation. Unnecessary packet generation can be suppressed with the repeated or almost similar observations.

• Reliability-Aware Aggregation

ARSDA gives a reliability value to each node based on the consistency of its observations. Reliability score is calculated as in eq.5:

(5)

where is the reliability score for sensor is the observed deviation from (4), is the sensitivity parameter that sets the acceptable deviation and e is the exponential constant. Therefore, those reading behaviors that are near the expected receive a higher reliability score and those that are inconsistent receive a lower score. Reliable observations from neighbouring nodes are aggregated using reliability-weighted aggregation at the aggregator as follows in eq.6:

(6)

where is the value that is obtained after aggregating the value of the aggregator with values from m valid reading member nodes is the value generated by member is the reliability score of Thus, more consistent sensor readings have a greater impact on the overall aggregate than do unreliable sensor observations.

• Reliability-Energy-Aware Forwarding

The basic method of WRDAS assigns the node priority based on the node energy, distance to the sink and neighbourhood information before TDMA scheduling. ARSDA takes this concept one step further, adding sensing reliability. The forwarding priority of node S_i is given by:

(7)

where is the forwarding priority, is the current residual energy, the initial energy, is the reliability, is the data similarity/aggregation quality, is the node-to-sink distance, and is the maximum considered communication distance. The relative contribution of energy, reliability, aggregation quality and distance are controlled by the coefficients α, β, γ and δ. The higher the P_i, the better the node is for forwarding. Then TDMA scheduling is applied to selected nodes to minimize simultaneous transmission and packet conflict.

• Secure Data Aggregation

Local redundancy reduction is followed by security, which means that less packets need cryptographic protection. Based on a secure aggregation technique of the underlying RSDA scheme, which relies on EC-ElGamal for confidentiality and secret sharing for integrity, ARSDA secures information before it is multi-hop transmitted. A small integrity verification value is shown as in eq.8:

(8)

Here, is an integrity verification value computed by aggregator is a cryptographic hash function, is the aggregated reading, ID_j is the unique ID of the aggregator, and is the current time stamp, and ‖ is a concatenation operation. The timestamp can be used to help identify stale or replayed data, and the verification value can help the BS determine if the aggregated data has been modified.

• Results and discussion

The comparison of network performance of ARSDA with LEACH, WRDAS and RSDA is shown in Table 3. The minimum energy consumption obtained by ARSDA is 43.7 J with minimum end to end delay of 51.8 ms. It attains a 98.1% packet delivery ratio, 97.2% goodput and the maximum network lifetime of 1780 rounds. The reliability-energy-based forwarding, the redundancy suppression, and the controlled transmission scheduling are the causes of these improvements, since they help to minimize redundant communications and energy consumption.

Table Network Performance Comparison

Method	**Energy Consumption (J)**	**End-to-End Delay (ms)**	**Packet Delivery Ratio (%)**	**Network Lifetime (Rounds)**	**Goodput (%)**
LEACH	68.4	84.6	91.8	1180	88.7
WRDAS	51.2	62.5	95.6	1540	94.1
RSDA	56.8	69.3	96.2	1475	93.8
Proposed ARSDA	43.7	51.8	98.1	1780	97.2

The evaluation of data aggregation and reliability performance is represented in table-4. The aggregation ratio of ARSDA is 82.6%, and it can cut the redundant sensor information by 80.4%. The adaptive EMA-based filtering and reliability assessment give the rate of outlier detection as 96.3% and the accuracy of data as 98.2%. With such an combination between reliable observation selection and similarity based aggregation, coupled with scheduled forwarding, the packet loss rate is 1.9%, versus 8.2% with LEACH, proving beneficial.

Table Data Aggregation and Reliability Performance

Method	**Aggregation Ratio (%)**	**Redundancy Reduction (%)**	**Outlier Detection Rate (%)**	**Data Accuracy (%)**	**Packet Loss Rate (%) ↓**

LEACH	61.5	58.2	72.4	90.6	8.2
WRDAS	68.7	65.1	78.6	93.8	4.4
RSDA	71.3	68.5	83.2	95.1	3.8
Proposed ARSDA	82.6	80.4	96.3	98.2	1.9

The security overhead and resource overhead of the methods evaluated are shown in Table 5. ARSDA can reach a 98.3% security success rate, 98.6% data integrity and only 10.8KB per round communication overhead. It has a security energy cost of 5.4 J which is less than the compared schemes. The application of security after local redundancy reduction reduces the amount of information that needs to be protected, therefore controlling the communication and cryptographic processing overhead in the resource-constrained sensor nodes.

Table Security and Resource Overhead Comparison

Method	**Security Success Rate (%)**	**Communication Overhead (KB/Round)**	**Computation Time (ms)**	**Security Energy Cost (J)**	**Data Integrity (%)**
LEACH	72.5	18.6	14.8	8.4	84.3
WRDAS	80.7	15.4	13.1	7.2	89.5
RSDA	96.8	13.2	18.7	6.5	97.4
Proposed ARSDA	98.3	10.8	15.2	5.4	98.6

• Conclusion, limitation and future scope

WSN still have to deal with various problems such as limited energy resources, redundant data transmission, communication reliability, and secure information delivery. Thus, it is necessary to have an effective data aggregation for reducing the network traffic at the same time maintaining the accuracy of the data and prolonging the lifetime of the network. This paper proposed Adaptive Reliability-Aware Secure Data Aggregation (ARSDA) framework to resolve different challenges such as energy consumption, redundant sensing, unreliable observations, communication overhead, and data security in resource-limited WSNs. ARSDA is a hybrid of EMA-based filtering and adaptive deviation assessment to detect and remove redundant and abnormal observations prior to transmission. Reliability-weighted aggregation retains valuable sensor data, and a combined reliability-energy priority mechanism takes into account the residual energy, data reliability, aggregation quality and communication distance when choosing the forwarding nodes. The TDMA-based scheduling also reduces collisions and unnecessary retransmissions of packets. The local data reduction is followed by secure aggregation that ensures both confidentiality and integrity of data but avoids excessive communication overhead. A simulation-based evaluation of ARSDA versus LEACH, WRDAS and RSDA was done on network, aggregation, reliability and security measures in OMNeT++. ARSDA reached a packet delivery ratio of 98.1%, data accuracy rate of 98.2%, and prolonging the network lifespan to 1780 rounds. The packet loss rate was brought down to 1.9%, as well. These findings suggest that integrating sensing reliability, energy availability, redundancy, forwarding distance and security can be beneficial in utilizing resources when compared to considering each of these requirements individually. Thus, ARSDA offers a viable data aggregation solution for resource-constrained WSN applications that have need for reliable and secure data delivery.

The presented assessment is completed for a static WSN topology, fixed communication range, simulation-type experiments, and a single base station that is stationary. Mobility of nodes, heterogeneous energy capacities, varying channel conditions, and large-scale deployments are still issues to be investigated. Further research will assess ARSDA with physical testbeds of sensors and mobile WSN scenarios. Energy-harvesting nodes, lightweight attack detection, adaptive security levels and larger network configurations can also be considered to evaluate ARSDA under realistic deployment scenarios.

References

- G. Adiline Macriga, K. Malarvizhi, S. Sobitha Ahila, N. K. Babu C, S. Ayyasamy, and B. M. Yashaswini, “Energy efficient greedy tree based algorithm for data aggregation in wireless sensor network,” Measurement: Sensors, vol. 30, p. 100910, 2023, doi: https://doi.org/10.1016/j.measen.2023.100910.
- Y. Song, S. Zhang, and S. Wang, “An energy efficient fusing data gathering protocol in wireless sensor networks,” Computer Networks, vol. 243, p. 110305, 2024, doi: https://doi.org/10.1016/j.comnet.2024.110305.
- K. Zhang, G. Zhang, X. Yu, S. Hu, and M. Li, “Clustering the sensor networks based on energy-aware affinity propagation,” Computer Networks, vol. 207, p. 108853, 2022, doi: https://doi.org/10.1016/j.comnet.2022.108853.
- P. Suman Prakash, D. Kavitha, and P. Chenna Reddy, “Delay-aware relay node selection for cluster-based wireless sensor networks,” Measurement: Sensors, vol. 24, p. 100403, 2022, doi: https://doi.org/10.1016/j.measen.2022.100403.
- M. Saadati, S. M. Mazinani, A. A. Khazaei, and S. J. S. M. Chabok, “Energy efficient clustering for dense wireless sensor network by applying Graph Neural Networks with coverage metrics,” Ad Hoc Networks, vol. 156, p. 103432, 2024, doi: https://doi.org/10.1016/j.adhoc.2024.103432.
- G. Vennira Selvi, V. Muthukumaran, A. C. Kaladevi, S. Satheesh Kumar, and B. Swapna, “Integrated dominating and hit set-inspired unequal clustering-based data aggregation in wireless sensor networks,” International Journal of Intelligent Computing and Cybernetics, vol. 15, no. 4, pp. 642–655, 2022, doi: https://doi.org/10.1108/IJICC-10-2021-0225.
- B. G. Sheena and N. Snehalatha, “An efficient energy consumption model using data aggregation for wireless sensor network,” International Journal of Communication Systems, vol. 36, no. 9, p. e5471, Jun. 2023, doi: https://doi.org/10.1002/dac.5471.
- F. Yang, Z. Xu, and L. Yang, “An efficient dual layer data aggregation scheme in clustered wireless sensor networks,” ETRI Journal, vol. 46, no. 4, pp. 604–618, Aug. 2024, doi: https://doi.org/10.4218/etrij.2023-0214.
- K. Jain and S. Kumar, “Integrating Blockchain and Machine Learning for Secure Data Aggregation in Wireless Sensor Networks,” International Journal of Communication Systems, vol. 38, no. 16, p. e70259, Nov. 2025, doi: https://doi.org/10.1002/dac.70259.
- K. Jain and A. Singh, “A two-vector data-prediction model for energy-efficient data-aggregation in wireless sensor network,” Concurr Comput, vol. 34, no. 11, p. e6898, May 2022, doi: https://doi.org/10.1002/cpe.6898.
- Z. Liu, J. Zhang, Y. Liu, F. Feng, and Y. Liu, “Data aggregation algorithm for wireless sensor networks with different initial energy of nodes,” PeerJ Comput Sci, vol. 10, p. e1932, 2024, doi: 10.7717/peerj-cs.1932.
- Z. Zhang, W. Yang, F. Wu, and P. Li, “Privacy and integrity-preserving data aggregation scheme for wireless sensor networks digital twins,” Journal of Cloud Computing, vol. 12, no. 1, p. 140, 2023, doi: 10.1186/s13677-023-00522-7.
- Heidari, H. Shishehlou, M. Darbandi, N. J. Navimipour, and S. Yalcin, “A reliable method for data aggregation on the industrial internet of things using a hybrid optimization algorithm and density correlation degree,” Cluster Comput, vol. 27, no. 6, pp. 7521–7539, 2024, doi: 10.1007/s10586-024-04351-4.
- Begum and S. v Nandury, “Data aggregation protocols for WSN and IoT applications – A comprehensive survey,” Journal of King Saud University Computer and Information Sciences, vol. 35, no. 2, pp. 651–681, 2023, doi: 10.1016/j.jksuci.2023.01.008.