



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 1, January 2022

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 7.569

9940 572 462

6381 907 438

[ijirset@gmail.com](mailto:ijirset@gmail.com)

[www.ijirset.com](http://www.ijirset.com)

# Data Aggregation Strategies in Wireless Sensor Networks for Efficient Communication

SURESH B

Senior Scale Lecturer, Government Polytechnic Koppal, Karnataka, India

**ABSTRACT:** A wireless sensor network consists of a large deployment of sensor nodes across a geographical area. Recent advancements in wireless communication and electronics have led to the development of low-cost wireless sensor networks (WSNs). When radio applications are considered, the sensor nodes sense the data and broadcast the sensed data to the destination or access point. A well-designed routing protocol is thus essential to reduce the energy consumption. In this study, we propose a Cycle-Based Data Aggregation Scheme (CBDAS) for grid-based WSNs. In CBDAS, the whole sensor field is divided into a grid of cells, each with a head. In most applications, the sensor nodes are powered using batteries which are not rechargeable. In addition, the power consumption analysis for individual sensors and cluster heads is performed that considers the communicational and computational cost as well. Simulation of our proposed method reveals quality performance than existing data aggregation method based on wavelet entropy and entropy based data aggregation protocols respectively. The evaluation criteria include—cluster head survival, aggregation cycles completed during simulation, energy consumption and network lifetime. In remote applications, it is even impossible to replace the batteries. It is believed that closely spaced sensor nodes sense data that are spatially correlated. Thus redundancy exists in the data, which can be removed by data aggregation. The amount of data transmitted to the access point is thus reduced and the transmission cost is also reduced.

**KEYWORDS:** wireless sensor networks (WSNs), Based Data Aggregation Scheme (CBDAS), criteria include—cluster head, consumption analysis, geographical area.

## I. INTRODUCTION

In wireless sensor networks (WSNs), the transmission data collected by the sensor nodes will be classified as different types. The data are homogeneous if they have the same properties; otherwise, they are heterogeneous data with different properties. In practical applications, the requirements for the data are always heterogeneous such as image, video, and multidimensional big data. The requirements for the heterogeneous data-transmitting function are often for special purposes, because the heterogeneous data are multidimensional data. In the process of data transmission, aggregating the data from the subnodes is called the data aggregation technology. The nodes in networks are heterogeneous for the network extensive applicability: the nodes have different energies, functions, communication abilities, and so on. Some nodes in the network are endowed with stronger ability to enhance the network communication ability, which are called supernodes. The core idea of topology control in the WSNs is to ensure the safety and reliable transmission of the collected data by the sensor nodes. The main method of maintaining the constructed network topology is to ensure the integrity of the maximum connected graph. In recent years, the requirements of the application fields of WSNs are continuously increasing. The topology structure is formed by self-organization network. Not only the complete communication but also the scalability and universality of the network are required in many cases. In other words, a topology is required to satisfy the requirements of various types of users.

## II. LITERATURE REVIEW

**Ahmad S. Abdullah (2021)** Recent advances in wireless sensor networks (WSNs) have inspired various new applications, including target tracking and monitoring of ecosystems. Nevertheless, a large amount of data energy consumption of WSNs is utilized by data communication. However, data aggregation techniques can eliminate redundant data being transferred back to the base station and thereby lessening the consumption of energy. Security features like data integrity, confidentiality and accumulation of latest data is of great importance if WSN is utilized in extremely hostile or remote settings whereby the sensors are vulnerable to node failure and breach. Currently, there is prospect for securing data aggregation using WSN. In light of this, security features in data aggregation using WSN will be examined in current study. Next, the adversarial model that can be used in any aggregation scheme is then evaluated.

**Zhaohui Zhang (2020)** Aiming at the transmission of heterogeneous data in heterogeneous networks, a topology optimization algorithm of heterogeneous wireless sensor networks based on local tree reconstruction is proposed, which can achieve better data transmission in the heterogeneous networks. First, the algorithm divides the nodes of the network into different layers by their hops and chooses different numbers of nodes as relay nodes in different layers. Second, the nodes are set with different initial energies in different layers. Because the packets of different nodes have different sizes, we adopt the corresponding data aggregation coefficients according to the actual data requirements of the network in data transmission. The simulations indicate that after the aforementioned three steps, the proposed algorithm prolongs the lifetime of the heterogeneous networks and improves the nodes utilization effectively.

**Mandeep Kaur (2020)** In recent years, wireless sensor network (WSN) is one of the rapidly growing area in various domains such as disaster relief operation, military applications, health applications, etc. In WSN, to eliminate the redundant information from the gathered data, data aggregation is a prime approach by which we can considerably reduce the energy consumption of each node. This reduction supports the achievement of the higher lifetime of WSN. In this study, we have endeavored to introduce a review of various existing data aggregation algorithms in the literature. We have also tried to summarize all these existing data aggregation algorithms on the basis of different performance metrics such as energy consumption, network lifetime, delay, energy cost, etc. Finally, this study supports the reader an idea to select the data aggregation algorithm for the desired application.

**Sabrina Boubiche et al (2018)** The emergence of new data handling technologies and analytics enabled the organization of big data in processes as an innovative aspect in wireless sensor networks (WSNs). Big data paradigm, combined with WSN technology, involves new challenges that are necessary to resolve in parallel. Data aggregation is a rapidly emerging research area. It represents one of the processing challenges of big sensor networks. This paper introduces the big data paradigm, its main dimensions that represent one of the most challenging concepts, and its principle analytic tools which are more and more introduced in the WSNs technology. The paper also presents the big data challenges that must be overcome to efficiently manipulate the voluminous data, and proposes a new classification of these challenges based on the necessities and the challenges of WSNs.

### Data Aggregation in WSNs

The significant purpose of data aggregation schemes in WSNs, is to collectively accumulate the data in an energy efficient way. The collected data has to be processed before arriving at the Base Station (BS). At the BS, necessary action is taken depending on the information collected by these tiny sensors deployed in the region of interest. For certain applications the data outcome is really massive as well as redundant. The redundancy is introduced because of the correlation, which exists among the collected data. The end objective at the BS is to take necessary action, from the sensors with minimal amount of collected data, which in return enhances the life span of the network. Collection, processing and delivery of the sensor data are to be managed in an efficient way. When the purpose to achieve is, an energy-efficient data collection without compromising the fidelity of the recovered data then data, aggregation methods play a very important role.

### Security in WSNs

The sensor networks deployed for mission-critical tasks, such as military applications must employ certain security needs during its design. In wireless system, it is easy to extract information, which results in a leakage of information as well as chance of eavesdropping and packet inflow by an adversary. Thus security to WSN to ensure secrecy and privacy of the data has to be properly addressed. One of the major internal attacks is, node compromise, by which an adversary can inject an internal attack. A Compromised Node (CN) attack is an attack in which an adversary compromises a certain subset of nodes to passively intercept data packets traversing the compromised nodes.

### Data Aggregation using CS

Data gathering in an energy efficient way is one of the important requirements in WSNs. With incorporation of CS, as a data aggregation scheme the information contained in the signal is safely maintained through its projections which can be reconstructed later. Inclusion of CS for an energy efficient routing technique further enhances the lifetime of the network. The dimensionality reduction at the transmitter is carried out using a measurement matrix. At the receiver data is recovered using reliable CS recovery methods. Depending upon the need of the application, suitable recovery methods can be applied. The reconstruction errors vary depending upon the reconstruction methods. Greedy based recovery methods are more popular, because of its low complexity and low implementation cost. Identification of correct basis is an essential requirement as the signal may not be sparse in the acquired domain.

### Energy-efficient and reliable data collection in WSNs

In the literature, there are various contributions towards security in WSNs. An authenticated group key agreement (AGKA) protocol, and demonstrates how it can tackle node replication and Sybil attacks. Efficient and secure routing protocol based on encryption and authentication. This method involves encryption of all communicated packets. In reliability is achieved through re transmissions. Dong proposed a routing scheme called Reliability and Multipath Encounter Routing (RMER), to achieve reliability and energy efficiency. The first major contributions to the secure reliable data collection of sensor networks started with H-SPREAD, which used Shamir Secret Sharing (SSS) schemes to generate multiple shares of the data. Additionally, a hybrid multipath scheme was used to route the shares. However, the achieved security was low, because fixed multipath were used to send the data. In addition, the presence of an adversary near the BS was not considered in their approach.

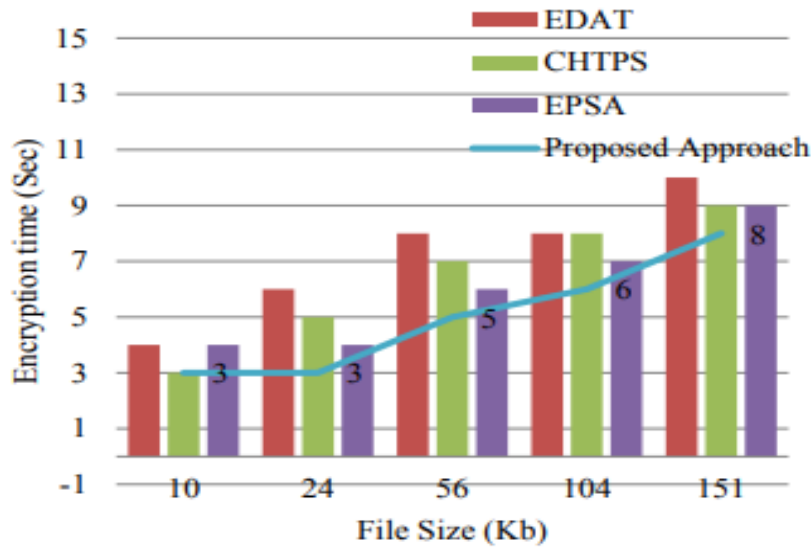
### III. RESEARCH METHODOLOGY

A network is originally founded with vertices and nodes densely interconnected. Following network formation, a method known as clustering is carried out in which nodes are split up into various clusters. Every cluster agent transmits data to a central, decrypting it using the proper key. The base station searches for missing data and uses a perfecting backup system to find it. The clustering agent is chosen from each group of interconnected clusters after the collections have been generated based on energy, proximity to the access point, and neighboring nodes. Each node gets a key from the base station, which also transmits keys to the other nodes. Generating routes from each node to the access point is to be done. Each node transmits data to its cluster agent after analyzing the hash value on-site. Cluster agents gather all the data and ensure that it is accurate. The clustering agent confirms the validity of the data before concluding the data aggregation procedure. Data to the access point, too. The suggested methodology represents a system's flow. First, an infrastructure of sensor nodes is established. Next, a clustering algorithm is applied, and the number of sensor nodes is partitioned into clusters. A cluster agent is then chosen based on three criteria. Key distribution is then carried out with each node via the base station, and a route is then produced from every node to the BS. Secure the data using the secret key and the elliptic curve ElGamal (ECE) algorithm. The encrypted data's hash value is determined, and a timestamp is noted. Each cluster's cluster agent receives data from the cluster member. Data is validated using its hash value; if validated, it is accepted; else, it is discarded. Then combine every data from the node and send it to the BS. Using the proper keys, the central server decodes the data.

### IV. RESULTS AND DISCUSSION

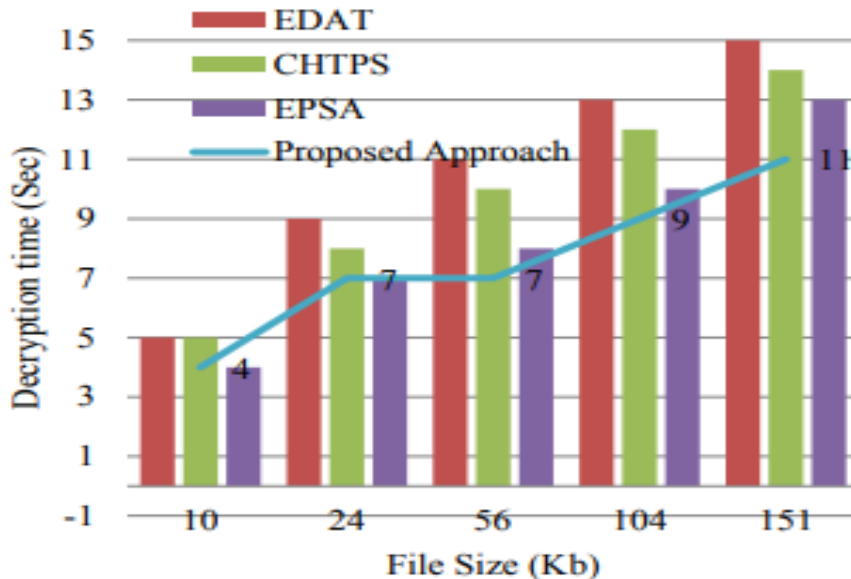
The effectiveness assessment is carried out to see how well the suggested procedure performs compared to other protocols. NS-2 is the simulation platform that is most frequently utilized. The suggested protocol's performance analysis is simulated using a network simulator. This section begins by providing a succinct definition of measuring performance. The effectiveness of the results is comparable to that of the CH Trust Propagation Scheme (CHTPS) and the Efficient and Provably Secure Aggregation (EPSA) protocols.

According to the current research, the strategy is carried out on a computer system with an Intel Core i5 CPU running at 2.66 GHz and 4 GB of RAM.



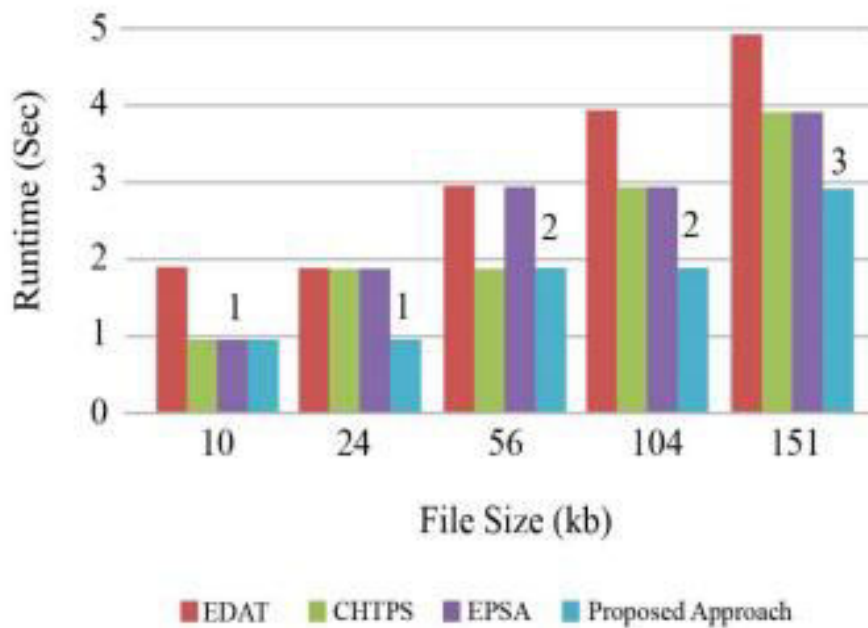
Graph 1: Encryption time

Although the CPU performs quicker than actual sensor nodes, it can still be utilized to show how well-allied approaches perform. The encrypt, decrypt, aggregate, and overall calculation time of the proposed and conventional techniques are displayed in Graphs 1, 2, and 3 accordingly.



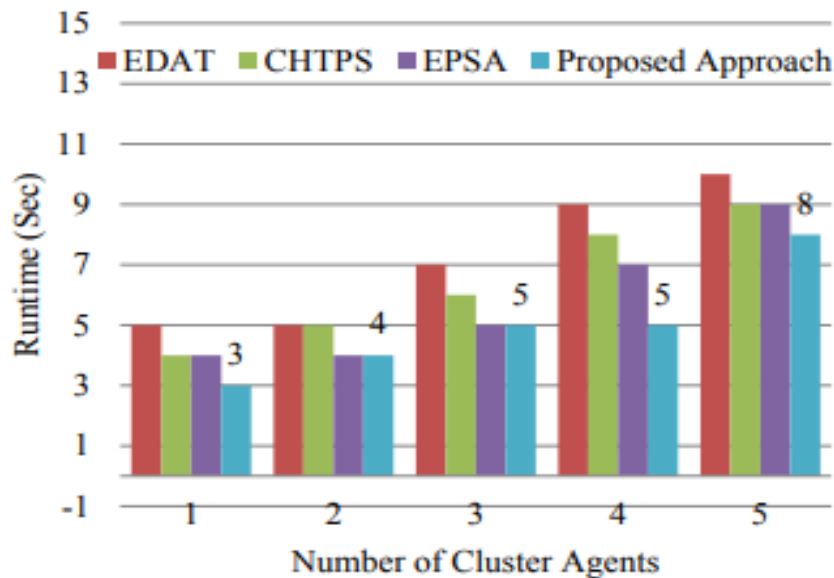
Graph 2: Decryption time

The suggested methodology is compared with the previous algorithm using several estimating criteria, such as the Efficient Data Aggregation Technique (EDAT) design and the Efficient and Provably Secure Aggregation (EPSA) method.



Graph 3: Aggregation time

In contrast, Graph 4 depicts the whole calculation time for a single cluster agent, changing sensor nodes. The energy used for varying the sensor nodes and the calculation time is directly correlated.



Graph 4: Overall processing time when the cluster agents are changed

Display the total computational effort for 20 sensor nodes, 10 kB of file size, and changing the cluster Agents. As SIES lacks an aggregate signature, it requires additional calculation time in both scenarios. Because EPSA includes more header information at each level, it takes longer to compute in both scenarios.

## V. CONCLUSION

In the current study, secure information aggregating encrypted files is accomplished on WSNs. At the same time data Security and validity are guaranteed by composite authentication. Data secrecy is given through the use of encryption.

Despite the higher expense, aggregate verification is still appropriate for WSNs. In the process of topology optimization, this research adopts three steps to adjust the structure of the network. The network has a strong topology after the three steps of the network topology optimization. Data aggregation aids in reducing the number of messages transmitted within the network, which in turn lowers total network energy consumption, by examining the effectiveness of data aggregation in this research. To solve this problem, the system provides a method in which an efficient cluster agent is preferred depending on their location for the access point and energy availability. The simulation results of the proposed algorithm have higher performance and reduce the energy consumption of the nodes in the network effectively under the same simulation conditions and parameters. The data transfer in heterogeneous networks contains different types of data, which include two-dimensional data, audio, image, and video. These data extremely demand for good network topology, so it is difficult to realize the transmission requirements of these data in homogeneous networks. Usually, the size of heterogeneous data packets is very large. The tree-based sensor network topology proposed in this paper only considers the data transmission between link layers. Furthermore, for the reason of technical difficulty, in this study, we have not studied the optimization problem under the data-sending rate and it is necessary to study this problem in the data transmission-based network.

#### REFERENCES

1. S. Boubiche, D. E. Boubiche, A. Bilami and H. Toral-Cruz, (2018) "Big Data Challenges and Data Aggregation Strategies in Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 20558-20571, doi: 10.1109/ACCESS.2018.2821445.
2. Mandeep Kaur (2020), "Data aggregation algorithms for wireless sensor network: A review", Ad Hoc Networks, ISSNno:1570-8713, Vol.100, <https://doi.org/10.1016/j.adhoc.2020.102083>
3. Giuseppe Anastasi (2009), "Energy conservation in wireless sensor networks: A survey", Ad Hoc Networks, ISSNno:1570-8713, Vol.7, Issue.3, Pages.537-568. <https://doi.org/10.1016/j.adhoc.2008.06.003>
4. Zhaohui Zhang (2020), "Data Aggregation in Heterogeneous Wireless Sensor Networks by Using Local Tree Reconstruction Algorithm", Complexity, ISSN no:1099-0526, Vol.2020, <https://doi.org/10.1155/2020/3594263>
5. Chih-Hung Hsieh (2014), "A Cycle-Based Data Aggregation Scheme for Grid-Based Wireless Sensor Networks", Sensors, ISSNno:1424-8220, Vol.14 (5), Pages.8447-8464. <https://doi.org/10.3390/s140508447>
6. geographical area (2006), "Data aggregation techniques in sensor networks: A survey", Electrical Engineering and Computer Science, ISSNno:2287-106X, Vol.22,
7. Prasun Sinha (2006), "Data Aggregation in Wireless Sensor Networks", Wireless Sensor Networks and Applications, ISSNno:2278-0181, Pages.331-347. [https://doi.org/10.1007/978-0-387-49592-7\\_13](https://doi.org/10.1007/978-0-387-49592-7_13)
8. Ahmad S. Abdullah (2021), "Review on secure data aggregation in Wireless Sensor Networks", IOP Conference Series: Materials Science and Engineering, ISSNno:1757-899X, Vol.1076, DOI:10.1088/1757-899X/1076/1/012053



**Impact Factor:  
7.569**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details