Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Efficient and Sustainable Utilizations of Sensor Networks with Minimal Traffic Using K-Medoid based Hybrid Clustering

Dr. E. Sreedevi[1], Dr. Ravikiran K[2], G. Siva Sankar[3], Dr. Bechoo Lal[4], Sindhuri Suseela Mantena[5], Dr. K. Aruna Bhaskar [6,*]

[1,4,6]Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation (KL University), Vaddeswaram, A.P.
[2]Department: IT, Gokaraju Rangaraju Institute of Engineering and Technology. Hyderabad, Telangana.
[3]Department of AI&ML, Aditya University, Surampalem, A.P- 533437, India
[5]Department of Computer Science and Technology, SRKR Engineering College, Bhimavaram, A.P, India
sridevi_fed@kluniversity.in[1], ravi.10541@gmail.com[2], sivacse517@gmail.com[3], drblalpersonal@gmail.com[4], mantenaa.suseela@gmail.com[5], arunabhaskar@kluniversity.in[6]

ARTICLE INFO

Received: 14 Dec 2024

Revised: 20 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The network traffic is one of the significant research issues in current communication industries due to people are passing bulk and unwanted data to transmit from one network segment to another network segments. Efficient and sustainable utilisation of sensor networks necessitates minimal traffic within the networked sensors (WSNs). These networks comprise multiple sensor nodes that are interconnected, and their optimal performance is achieved through the avoidance of congestion, low energy consumption, elimination of duplicate information transmission, and minimal data transfers to the sink. Efficient attainment of these objectives necessitates the use of data aggregation. The principal objective of data aggregation is to effectively collect and merge data, while simultaneously eliminating superfluous data in order to improve the longevity of the network. This study's review centered on various information aggregation methods, such as flat networks, hierarchical systems, and structure-free systems, and their respective variations. The current research centres on the initiation of work pertaining to energy-efficient data collection and the administration of large databases through the utilisation of distinct models such as K-medoid, k-means, and fuzzy-based clustering mechanisms for validation. The objective is to enhance data collection in wireless sensor networks, thereby demonstrating an improved cluster head selection rate and a better minimum distance rate between two nearby nodes through the proposed scheme. Overall, the implementation of the proposed scheme yields a performance improvement of more than 13 to 17% when compared to the results obtained from the current system.

Keywords: Wireless Sensor Networks, K-medoid, k-means, fuzzy-based clustering mechanism, Sensor nodes, Base station.

INTRODUCTION

The utilisation of WSNs, or wireless sensor networks, has gained significant traction and relevance across diverse domains. Wireless Sensor Networks (WSNs) typically exhibit redundancy in their data. As a result of this phenomenon, data emanating from distinct sensor nodes are consolidated prior to transmission to the central station. The practice of aggregating information is utilized to prevent the superfluous transmission of data. Efforts have been dedicated towards enhancing communication efficiency due to the fact that data transmission results in heightened energy consumption. This gives rise to several security concerns [13].

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Wireless Sensor Networks (WSNs) are expected to possess extended network lifespan due to their restricted electrical power and communication capabilities. The primary objective is to minimize energy consumption, with the main goal being to extend the network's lifespan. Wireless sensor networks consist of diminutive sensor nodes that are utilized for detecting, processing of data and aggregation, as well as communication components. Data aggregation is an essential component in Wireless Sensor Networks (WSN) as it helps to mitigate energy consumption resulting from excessive communication [32][33]. Wireless sensor networks have a variety of applications, including but not limited to building tracking, a home tracking, military surveillance, health monitoring, and target tracking [34].

A wireless sensor network, or WSN, comprises of numerous sensors that collect data and transmit it to a designated base station, as illustrated in Figure 1. There exist various applications for Wireless Sensor Networks (WSN), including but not limited to industrial applications such as machine monitoring and control, healthcare analysis. Within the final category, there exist numerous protocols such as DD, SPIN, and SAR. The initial classification comprises a plethora of protocols such as TEEN, LEACH, and others [19]. lightweight security methods that are suited for WSNs with limited resources and guarantee data integrity without putting undue strain on the nodes [20]. A thorough analysis of safe data aggregation with homomorphic encryption, which maintains privacy without sacrificing security by enabling data to be aggregated in its encrypted form. The assessment assesses current systems critically and points out unresolved research problems, including the requirement for lightweight cryptographic primitives appropriate for WSNs, significant computational cost, and scalability problems [21].

A two-tiered strategy that combines behavioral monitoring of sensor nodes with secure data aggregation to identify malicious activity. By spotting unusual communication patterns and separating infected nodes, their approach improves overall network resilience while guaranteeing data authenticity and network integrity [22]. Adaptive routing techniques are required to handle WSNs' dynamic and energy-constrained characteristics, particularly in mission-critical applications [23]. Even if any nodes malfunction or act maliciously, reliable data collecting is ensured by redundant data aggregation channels and error correction techniques [24].

The process of information gathering typically involves aggregating data from multiple sensors in order to eliminate redundant data packets and generate a single consolidated dataset for transmission to the base station. A data aggregation scheme is deemed energy-efficient when it enhances the efficacy of the network. The implementation of secure data aggregation ensures the security of the data aggregation process by requiring authentication of the aggregator, thereby enhancing the overall security of the system [25].

The network in question is unmonitored and lacks hardware that is resistant to tampering, owing to its significant features and wireless setting. This type of network is susceptible to various forms of attacks. A safe data accumulation technique is employed to ensure the safety of the entire network. The implementation of secure data aggregation ensures the provision of security to the process of data aggregation [26][27]. It is imperative to replace current methodologies with an enhanced approach that utilizes aggregation. In the context of data aggregation techniques, an aggregator node is responsible for selecting all relevant information from various sensor nodes and subsequently reducing the amount of data transmitted by transmitting partial results to the base station [28][29]. the importance of application-specific routing designs in WSNs. By aligning routing decisions with data characteristics and aggregation opportunities, networks can achieve better performance and longevity. This early work laid a foundation for many later protocols that prioritize data-centric aggregation and energy-aware routing [30].

In this technique utilized to enhance network longevity through the consolidation of data, utilizing metrics such as minimum, maximum, and average values to optimize energy consumption. Figure 1, Wireless Sensor Networks (WSNs) exhibit a high degree of sensitivity to data, thereby enabling adversaries to surreptitiously intercept the transmitted information. As an illustration, the malevolent party can acquire the information from the designated node by severing the connection between an originating node and a receiving node. Additionally, malevolent nodes possessing comparable attributes can gain entry into the network or alter the path of transmission. Therefore, the implementation of security measures is of utmost importance in order to maintain the integrity of a network. The implementation of security measures can present significant challenges, primarily due to limited energy resources and the imperative to minimize transmission overhead. Therefore, it is imperative to consider energy efficiency as a fundamental limitation [1].

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

This study aims to investigate in the present research. The implementation of a broadcast network utilizing a band-based bi-directional approach is proposed. By employing this methodology, information from sensors can be efficiently transmitted to the mobile sink while minimizing costs. The results of the simulations indicate that directional broadcast based on band offers superior performance when evaluated in terms of various parameters. The data in the band are directed towards the mobile sink without any collisions [2].

Sampling Initiation Signal

An additional sampling technique involves the transmission of SIS, which enables the process through broadcast within a specific range of samples. Consequently, it is possible to assign a label to the bands according to their geographical location, thereby facilitating the identification of the precise position of the utilized sensor and its efficacy. Upon receipt of an initiation signal, the sensor associated with the corresponding band undergoes mapping, while the remaining bands remain unaffected. Consequently, a limited number of detectors can be employed for the purpose of sampling, and this must be done in a methodical manner. The sample initiation signal comprises three distinct components, specifically the identifier for the sample signal, the identifier for the cell phone object in use, and the designated range of the band to be selected [3][4]. The selection and utilisation of sensors for sampling within a specific band can be determined based on the three aforementioned parameters.

Handling Packet Collisions: Data packets may experience collisions due to factors such as a sudden surge in data volume or a sudden reduction in time. The aforementioned problem can be resolved through the implementation of a band scheduling system for the deployment of sensors. Consequently, the simultaneous inundation of packets can be circumvented. Consequently, this will prevent instances of collision [5].

Upon reaching a certain threshold of operations, the system experiences failure. The term "DAC tree lifespan" refers to the duration of time that a DAC tree is able to exist. There are multiple factors that contribute to the malfunctioning of the nodes [6]. The node may either have encountered a failure in transmitting data to its parent node or it may be unable to retrieve information from its child nodes. In either case, a singular round is executed to gather the data that was not obtained during the occurrence of the failure. This process entails the collection of all data within the node during a single round, which commences from the lowest child and progresses towards its corresponding parent. The aforementioned data are stored within the reception sink [7].

Lein Harn et.al.,a(2021) proposed the principal objective of WSNs, or wireless sensor networks, is to gather diverse forms of data meteorological data, vehicular traffic data, and so forth. WSNs exhibit dissimilar characteristics compared to the data typically passed on in digital communication networks. The majority of data in wsntypically comprises a limited number of bits, whereas data in messaging uses tends to consist of a significantly larger number of bits. The data encryption methods currently employed in wireless sensor networks (WSNs). It is evident that traditional encryption methods are not appropriate for Wireless Sensor Networks (WSNs) due to the fact that the key sizes are significantly larger than the data sizes. Our study presents a new approach to data encryption that selectively encrypts a limited number of bits of data [8].

The security of this encryption method is established through the utilisation of multiple pair-wise key pairs with short lengths. The velocity of encryption is considerably higher in comparison to traditional symmetric encryption methods. The process of data aggregation has been identified as a highly effective means of transmitting data within a network [9]. Historically, the majority of encrypted data collection were developed utilizing homomorphism encryption based on public-key cryptography. Due to the computationally intensive nature of public-key encryption, its implementation is not considered appropriate for utilisationWSNs is transmitted via a route that traverses several sensor nodes, starting from the sending node and ending at the receiver node. Our proposed scheme enables sensors along the path to perform piggybacking when various information is gathered in Wireless Sensor Networks (WSNs) [10]. To minimize the size of the data packets, HC-LEACH incorporates Huffman coding into the data transmission phase. Sensor nodes use less energy when data is compressed before transmission, which increases the network's lifespan. The protocol greatly increases energy consumption efficiency, especially in data-dense situations, while preserving LEACH's fundamental clustering foundation [11]. The significance of cluster head selection and intelligent data handling in WSN energy conservation. These protocols make significant contributions to the development of

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

robust, sustainable sensor networks that are essential for a range of real-world uses, including military surveillance, smart agriculture, and environmental monitoring [12].

Encryption scheme has the following unique features:

The proposed encryption method has the capability to encrypt data using keys of short lengths. This is in contrast to most symmetric-key encryption techniques that require bit, such as a fixed block size of 128 bits in AES, and use a correspondingly large key size, such as 128/192/256 bits in AES. In our proposed encryption method, both the data and keys can be of very short lengths. As keys are generated through a random integer process, the level of difficulty in deciphering these keys is equivalent to that of decrypting the data itself. When the amount of data gathered is limited, the utilisation of shorter encryption keys results in a notably quicker process compared to the use of longer keys [13].

1. This differs from the typical approach of link-to-link encryption, which utilizes just one pair wise shared essential among sensors. The utilisation of multiple keys in data encryption can indeed augment its level of security [14].
2. The proposed encryption method exhibits a high speed due to its reliance on additions and subtractions, in contrast to the majority of symmetric-key encryption techniques that employ multiple rounds of bit string mixing. This encryption approach involves the utilisation of pair wise shared keys to add and subtract data strings [15].

Cong Pang et.al.,(2021) main aims to enhance energy efficiency and reduce processing delay. In order to facilitate the functioning of sophisticated applications, it is necessary for sensor nodes to transmit a variety of dissimilar and varied data. This requirement necessitates the need for multi-dimensional collection of information and versatile data analysis. In order to address the existing security concerns and functional necessities, we suggest a secure data aggregation approach that is both multi-functional and multi-dimensional [16]. Initially, a Chinese the rest theorem conversion technique is devised, incorporating a counter to encode information with multiple dimensions into large integers. This enables the utilisation of linear homomorphism data encryption schemes for operation purposes. Subsequently, a versatile data analysis technique is presented that facilitates a range of aggregation functions, such as linear, polynomial, and continuous functions. Furthermore, our study showcases that the suggested methodology can effectively attain [17]. Conserving data dependability while saving energy. This technique greatly aids in the creation of robust and sustainable sensor networks by streamlining the network's data processing and transmission [18].

METHOD

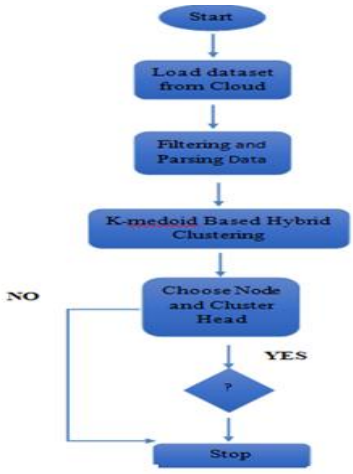


Figure 1: Proposed Research Study

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Steps:

Step1: In the initial step, data retrieval from the cloud is performed by employing the Matlab programmer function or an analogous cloud-based service such as mMatlabcloud or ThingSpeak.

Step 2: The second step involves the utilisation of the filtered and parsing concept to eliminate any uncertainty or noise present in the data.

Step 3: involves employing a hybrid methodology to determine the cluster centroid node and identify the optimal.

Step4: In the fourth step, data aggregation from S to D will occur if the chosen node possesses the qualities of trustworthiness, security, and energy efficiency.

Step 5: In the event that the chosen node does not meet the established criteria, proceed to select an alternative node.

Step 6: In accordance with Step 6, the CH node should be selected, and communication should be initiated accordingly.

The methodologies for data aggregation are typically categorized into two main groups: structure-free as well as structure-based data aggregation. The utilisation of a structure-based approach for data aggregation involves the implementation of various techniques such as tree-based, cluster-based, and hierarchical methods to effectively carry out the aggregation of data. The approach of aggregating data based on structure expends a significant amount of energy on the creation and upkeep of organized networks. In contrast, a data aggregation approach that is devoid of structure operates in a manner that conserves the energy necessary for constructing and up keeping the network. The event-driven approach is characterized by its reliance on network events to initiate its operations [2].

Data aggregation is a critical method for gathering data gathered by sensor nodes in wireless sensor networks (WSNs) due to the decentralized and dynamic nature of the network. The issue of power consumption is a critical consideration in the development of data aggregation protocols for wireless sensor networks, due to the high volume of repetitive data communication that occurs within these networks. Hence, the paramount consideration in the design of any Wireless Sensor Network (WSN) protocol is the efficient utilisation of energy resources [2].

The concept of energy efficiency refers to the ability to achieve a desired level of energy output while minimizing energy input. It involves the optimization of energy in an ideal scenario, it is expected that every sensor would consume an equal amount of energy during each data gathering round. However, in practical situations. The energy determined by its ability to offer optimal functionality while minimizing energy consumption. Energy efficiency can be defined as the ratio in the process of transferring that data. The utilization of Equation 1 is employed for the computation of energy efficiency**.**

$$\text{Energy Efficiency}i_i = \sum_{i=1}^{n}\left(\frac{\text{Amount of data successfully transferred in a sensor network}}{\text{Total energy consumed to transfer those data}}\right)$$

where n is the number of sensors nodes in a sensor network [33]. .....(1)

The Refers to the duration for which a network can operate effectively before its resources are depleted or the concept of network lifetime refers to the total number of information aggregation rounds that can be completed before the energy of the initial sensing node is depleted.

$$NL_n^n = \min_{v \in V} NL_v$$

NL_n^n= Life Time of Network

NL_v= Life Time of V Node

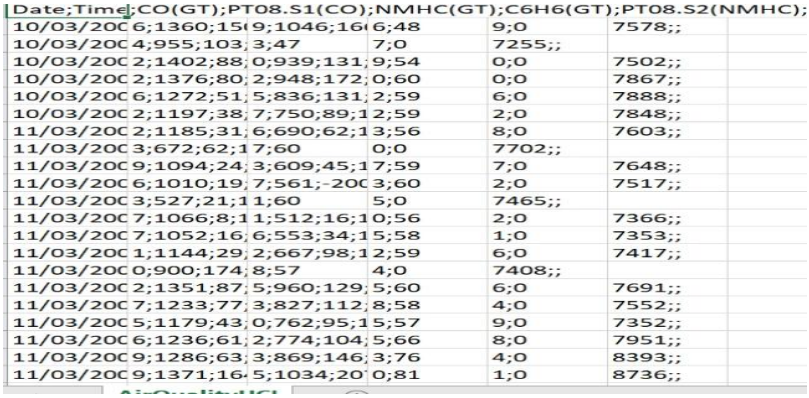
Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The subject matter under consideration pertains to the precision and reliability of data. The precise characterization of a network of sensors is contingent upon the particular context and purpose that the network is formulated. This concept is exemplified by the precise determination of the target's position at the washbasin, which plays a crucial role in assessing the accuracy of the data in the context of the entirety of transmitted information, as mentioned in the reference. The rate at which data is aggregated. DR is systematic gathering and consolidation of pertinent information within a specific area of interest. The process of data aggregation is regarded as a fundamental procedure for the purpose of minimizing energy consumption and conserving limited resources. It is defined in relation to the rate at which data is aggregated.

RESULTS

In this image use dataset and in dataset consider air quality data and consider different parameter like CO, NMHC, C6H6, PT08 etc.



Date;Time;CO(GT);PT08.S1(CO);NMHC(GT);C6H6(GT);PT08.S2(NMHC);				
10/03/20C	6;1360;15	9;1046;16	6;48	9;0	7578;;
10/03/20C	4;955;103	3;47	7;0	7255;;	
10/03/20C	2;1402;88	0;939;131	9;54	0;0	7502;;
10/03/20C	2;1376;80	2;948;172	0;60	0;0	7867;;
10/03/20C	6;1272;51	5;836;131	2;59	6;0	7888;;
10/03/20C	2;1197;38	7;750;89;1	2;59	2;0	7848;;
11/03/20C	2;1185;31	6;690;62;1	3;56	8;0	7603;;
11/03/20C	3;672;62;1	7;60	0;0	7702;;	
11/03/20C	9;1094;24	3;609;45;1	7;59	7;0	7648;;
11/03/20C	6;1010;19	7;561;-20C	3;60	2;0	7517;;
11/03/20C	3;527;21;1	1;60	5;0	7465;;	
11/03/20C	7;1066;8;1	1;512;16;1	0;56	2;0	7366;;
11/03/20C	7;1052;16	6;553;34;1	5;58	1;0	7353;;
11/03/20C	1;1144;29	2;667;98;1	2;59	6;0	7417;;
11/03/20C	0;900;174	8;57	4;0	7408;;	
11/03/20C	2;1351;87	5;960;129	5;60	6;0	7691;;
11/03/20C	7;1233;77	3;827;112	8;58	4;0	7552;;
11/03/20C	5;1179;43	0;762;95;1	5;57	9;0	7352;;
11/03/20C	6;1236;61	2;774;104	5;66	8;0	7951;;
11/03/20C	9;1286;63	3;869;146	3;76	4;0	8393;;
11/03/20C	9;1371;16	5;1034;20	0;81	1;0	8736;;

Figure 2: Dataset

Network Parameter	**Value**
Network size	200 m*200m
Number of Particle(k)	40
Maximum iteration	400
Numeral Node of Sensor	[60, 120]
Primary Energy (E0)	0.9 J
Sensing Range	[1,15] m

Table 5.2: Parameters

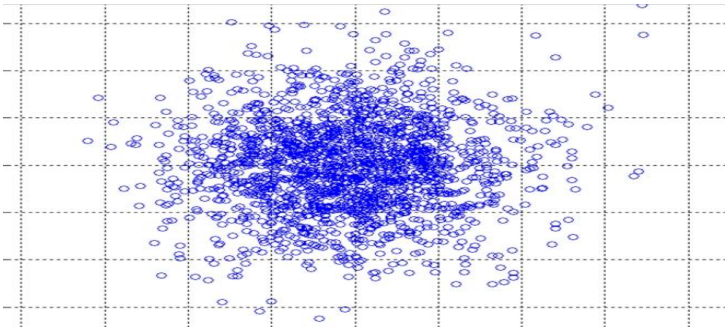


Figure 3: K-medoid clustering

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The application of k-medoid based clustering involves the partitioning of a given set of data points or objects into distinct classes, where each cluster consists of objects that share similar characteristics. This process entails dividing a group of n object.

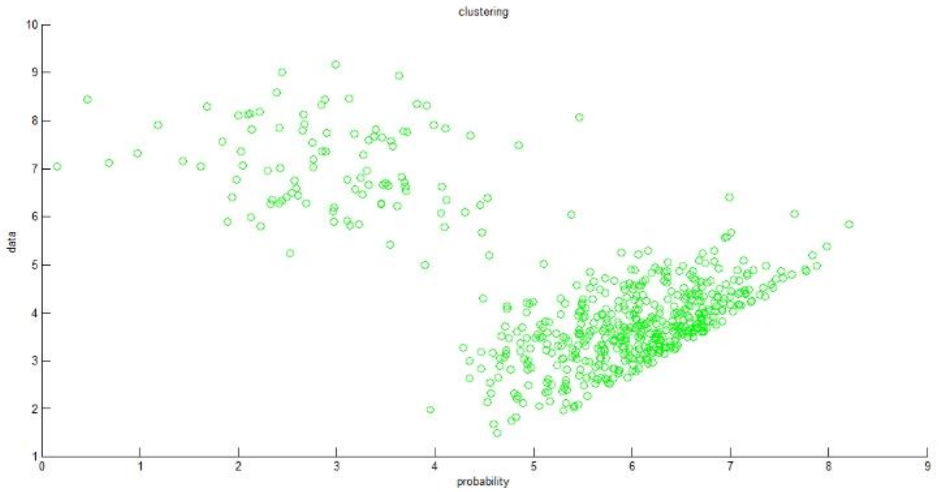


Figure 4: Clustering

Apply clustering mechanism and based on grouping and probability-based estimation create group of clusters.

2016-09-07 00:00:0	Overcast	rain	17.22222	17.22222	0.9	10.9158	351	16.1	0	1021.77	Partly cloudy throughout the day.
2016-09-07 01:00:0	Overcast	rain	17.22222	17.22222	0.9	11.0768	352	16.1	0	1021.87	Partly cloudy throughout the day.
2016-09-07 02:00:0	Mostly Clc	rain	17.20556	17.20556	0.93	10.6421	355	14.9569	0	1021.85	Partly cloudy throughout the day.
2016-09-07 03:00:0	Mostly Clc	rain	17.2	17.2	0.93	14.0231	11	14.9086	0	1021.69	Partly cloudy throughout the day.
2016-09-07 04:00:0	Mostly Clc	rain	17.17778	17.17778	0.93	14.0714	11	14.812	0	1021.49	Partly cloudy throughout the day.
2016-09-07 05:00:0	Mostly Clc	rain	16.70556	16.70556	0.97	13.3147	21	14.1197	0	1021.47	Partly cloudy throughout the day.
2016-09-07 06:00:0	Mostly Clc	rain	16.6	16.6	0.93	11.27	20	11.8979	0	1021.46	Partly cloudy throughout the day.
2016-09-07 07:00:0	Partly Clou	rain	17.15556	17.15556	0.93	12.9444	21	14.812	0	1021.37	Partly cloudy throughout the day.
2016-09-07 08:00:0	Partly Clou	rain	17.81111	17.81111	0.9	12.1555	22	13.7333	0	1021.36	Partly cloudy throughout the day.
2016-09-07 09:00:0	Partly Clou	rain	19.97778	19.97778	0.84	11.431	32	11.9784	0	1021.35	Partly cloudy throughout the day.
2016-09-07 10:00:0	Partly Clou	rain	22.71111	22.71111	0.71	11.1251	32	15.8263	0	1021.36	Partly cloudy throughout the day.
2016-09-07 11:00:0	Partly Clou	rain	23.88333	23.88333	0.66	10.4489	69	15.1501	0	1021.35	Partly cloudy throughout the day.
2016-09-07 12:00:0	Partly Clou	rain	26.01667	26.01667	0.55	9.499	79	16.1	0	1021.15	Partly cloudy throughout the day.
2016-09-07 13:00:0	Partly Clou	rain	27.66111	27.85	0.47	4.7012	103	15.8263	0	1020.65	Partly cloudy throughout the day.
2016-09-07 14:00:0	Partly Clou	rain	27.65556	27.61111	0.44	8.9033	105	15.3111	0	1020.31	Partly cloudy throughout the day.
2016-09-07 15:00:0	Partly Clou	rain	27.75556	27.75556	0.44	10.6582	177	16.1	0	1019.85	Partly cloudy throughout the day.
2016-09-07 16:00:0	Partly Clou	rain	28.79444	28.46111	0.41	7.4543	188	16.1	0	1019.55	Partly cloudy throughout the day.
2016-09-07 17:00:0	Partly Clou	rain	27.76111	27.42222	0.39	3.7674	141	15.5526	0	1019.36	Partly cloudy throughout the day.
2016-09-07 18:00:0	Partly Clou	rain	27.17222	27.23333	0.44	0.2737	125	16.1	0	1019.13	Partly cloudy throughout the day.
2016-09-07 19:00:0	Partly Clou	rain	23.83889	23.83889	0.62	3.22	70	16.1	0	1018.95	Partly cloudy throughout the day.
2016-09-07 20:00:0	Partly Clou	rain	21.00556	21.00556	0.73	0.322	10	15.5526	0	1019.43	Partly cloudy throughout the day.

Figure 5 Dataset_2

Network Parameter	**Value**
Network size	100 m*100m
Number of Particle(k)	20
Maximum iteration	200
Number of Sensor Nodes	[30, 60]

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Initial Energy (E0)	0.5 J
Sensing Radius	[3,13] m

Table 4.2: Parameters

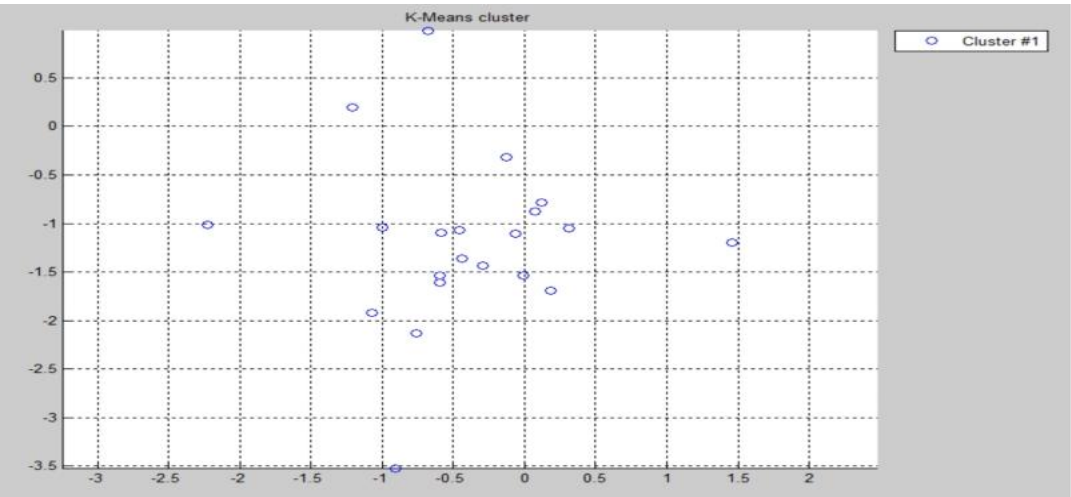


Figure 6: K-means clustering

1. Select a set of k random points, either from the given data set or from an alternative source. These points are alternatively referred to as "centroids" or "means".
2. The information points in the set of data are assigned their closest centroid by utilizing a distance formula such as Euclidean distance or Manhattan distance.
3. Next, the selection of new centroids is performed by calculating the median of all the data rewards within the clusters. This process is then followed by proceeding to step 2
4. Continue iterating step 3 until there are no data points that undergo a change in classification between consecutive iterations.

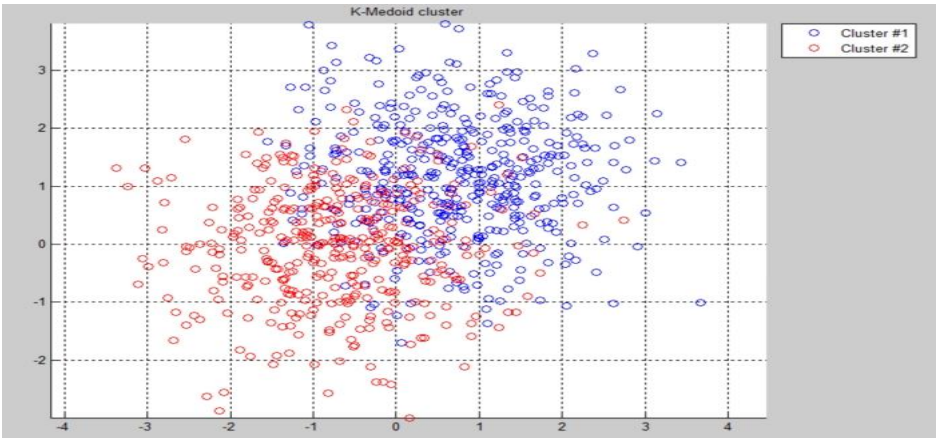


Figure 7: K-medoid clustering

A medoid refers to a specific point within a cluster that exhibits minimal dissimilarities when compared to all other points within the same cluster. In contrast to the utilisation of centroids as points of comparison in K-Means methods, the K-Medoids algorithm employs a Medoid as its reference point.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The data analyzing methodologies utilized by everyone data-driven model demonstrate variations. The query-driven model commences the initial stage with the creation of queries to extract data from sensors according to the user's defined needs. Once the user generates queries, the resulting query is then transmitted to the sensor nodes within the WSN. If the query is consistent with the data gathered by each sensor node, it is considered valid and approved. On the other hand, if the query result does not align with the existing data, it is ignored and subsequently eliminated. In a power source driven by events approach, sensor nodes predominantly function in a recognizing mode. Sensors commonly perceive data in reaction to a specific event, as well as upon the happening of said event, send the information to the fall node. In the absence of any detected event, the sensors persistently collect data without interruption. Within the framework of a time-dependent model, sensors were specifically engineered to consistently perceive and collect data. The sink node triggers a timer that prompts every sensor node to engage in data sensing. The sensor nodes divide the provided time interval into separate periods, which are subsequently further separated into smaller units referred to as slots. The transmission of data from the sensor nodes to a sink occurs within a predefined timeframe. In the event that this timeframe is not met, the sensor nodes will continue to collect data without interruption. Ultimately, a system that is hybrid is developed through the amalgamation of two distinct models. Suppose a hybrid strategy is created by integrating event-driven and time-driven models. In general, the hybrid model functions in tandem with a time-dependent model to periodically detect and transmit data. The hybrid model shifts from a time-influenced model to a driven by events model in order to enable efficient processing within wsn following the occurrence of an event

- The path-based detection algorithm is characterized by a node's observation of its immediate neighbor to the current route path, rather than monitoring all nodes in the neighborhood. In order to execute the algorithm, each node is responsible for maintaining a FwdPktBuffer, which serves as a buffer for packet digests. As the packet is being transmitted, its digest is added to a FwdPktBuffer, and the sniffing nodes intercept the communication. Upon the detection that the following node has successfully received the data packet, the processed version is subsequently released into the Sending Packet Buffer. The detecting node calculates the level of hearing for its neighboring node in the subsequent hop and subsequently evaluates it against a pre-established threshold. When the forwarding rate decreases to a level lower than the specified threshold cost, the detecting node classifies the subsequent hop neighbor to be a black hole and abstains from transmitting packets to the suspected nodes in subsequent occurrences.

$$OR\ (N) = \frac{total\ overhead\ packet\ number}{total\ forwared\ packet\ number} \quad \text{....(2)}$$

- The Exponential Trust-based mechanism involves the maintenance of a streak opposite (n) to monitor the consecutive dropping of packets. The utilisation of the black hole attack is predicated on the observation that all packets are deliberately discarded. A tolerance factor, denoted as X, is established to define the acceptable range within which the mechanism can operate in its designated environment. The trust factor in this mechanism is determined by utilizing the streak counter, which employs a formula that assigns a value of 100* to each node.
- The trust factor experiences an exponential decrease as a packet is dropped.
- The proposed mechanism integrates the protocol for AODV with reliability analysis to enhance the overall performance. The system includes a Data Rate Index (DRI) table that records the number of packets transmitted and received. The accuracy ratio of the path comprising the neighbouring nodes of node is determined based on the provided information.

$$Reliability\ Ratio = \frac{No.\ of\ packet\ sent}{No.\ of\ packets\ Received} \text{.....(3)}$$

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Additionally, the system includes a Reliable End-to-End Link (REL) packet that is transmitted once a dependable route has been identified. The REL packets are responsible for maintaining the reliability count for each individual node.

DISCUSSION

Finally the researcher concluded that propose an energy-efficient coverage control algorithm for WSNs based on Particle Swarm Optimization (PSO).In order to achieve a balance among coverage rate and cost of energy, the detection radius of every sensor node is adjusted with the objective of attaining this goal. So, for that, we design a proposed system that uses data aggregation using PSO with a k-medoid-based method for design and implements data transmission on low power and also energy efficiency. As the result showed proposed system will improve the energy efficiency of nodes and also improve the robustness of the system by detecting of malicious nodes. In future work on other routing protocols and also feature extraction methods like ACO and Honey bee. Wireless sensors are networks that operate under energy constraints. The optimization of data aggregation is a crucial concern due to the significant energy consumption associated with data transmission and reception. Efficient data collection not only contributes to energy conservation, but also eliminates redundant data, resulting in the provision of exclusively valuable data. When the data originating from a source node is transmitted to a sink node through neighboring nodes in a multiloop manner, with a reduction in spread and receiving authority, the resulting energy consumption is lower compared to the scenario where the data is sent directly to the sink node. This reduction in energy consumption is achieved through the process of data aggregation, which effectively reduces the amount of data transmission required.

REFRENCES

[1] Supriya H.S, Dr. Dayananda R.B, "Nearest Neighbor Monitoring Mechanism for Efficient and Secure Data Aggregation in WSN Environment", IEEE Xplore, 2021.
[2] Mamta R. Choudhari, Prof. Uday Rote, "Data Aggregation Approaches in WSNs", IEEE, 2021.
[3] Mr.D.Selvapandian, Dr.J.Joyce Jacob, Ms.R.Kannamma, Dr.R.Dhanapal, Dr.Jebakumar Immanuel.D, " An Efficient Bidirectional broadcasting using Signal Initiation and Data Aggregation for WSN", IEEE , 2020.
[4] Lein Harn, Ching-Fang Hsu, Zhe Xia, and Zhangqing He, "Lightweight Aggregated Data Encryption for Wireless Sensor Networks (WSNs)", IEEE, 2021.
[5] Cong Peng, Min Luo, Pandi Vijayakumar, Debiao He, Omar Said, Amr Tolba, "Multi-Functional and Multi-Dimensional Secure Data Aggregation Schemes in WSNs", IEEE, 2021.
[6] Gul Sahar, Kamalrulnizam Abu Bakar, Sabit Rahim, Naveed Ali Khan Kaim Khani and Tehmina Bi bi, "Recent Advancement of Data-Driven Models in Wireless Sensor Networks: A Survey", MDPI, 2021.
[7] Dr. Akella Amarendra Babu, Dr. G. Dileep Kumar, Dr. R. BalaMurali, Dr. K. Kondaiah, "Wireless S ensor Networks: Data Aggregation Using LEACH Routing Protocol", NCACNM, 2017.
[8] Naveen Kumar, Jyoti R. Desai, Dr. Annapurna D, "ACHs-LEACH: Efficient and Enhanced LEACH protocol for Wireless Sensor Networks", IEEE, 2020.
[9] C.Priyadarsini Dr.R.Prema, "Secure And Energy Efficient Data Aggregation Routing Protocol To Red uce Congestion in Wireless Sensor Network", IOSR-JCE.
[10] S. Sasirekha and S. Swamynathan, "A Comparative Study and Analysis of Data Aggregation Techniq ues in WSN", Indian Journal of Science and Technology, 2015.
[11] Djamila MECHTA, Saad HAROUS, "HC-LEACH: Huffman Coding-based energy-efficient LEACH protocol for WSN", IEEE, 2020.
[12] K.Muthukumaran,iiAsso.iiProf.,iDr.K.Chitra,iProfessor,iC.Selvakumar,iProfessor,i"EnergyiiEfficientiiClusteri ngiiInii WirelessiiSensoriiNetworks",iiIEEE,ii2017.
[13] V.Akila, Dr.T.Sheela, "Preserving Data and Key Privacy in Data Aggregation for Wireless Sensor Net works", IEEE, 2017.

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[14] Aishah Aseeri, Rui Zhang, "Secure Data Aggregation in Wireless Sensor Networks: Enumeration Attack and Countermeasure", IEEE, 2019.
[15] Ms. Sneha Ghormare, Mrs. Vaishali Sahare, "Implementation of data confidentiality for providing High Security in Wireless Sensor Network", IEEE, 2015.
[16] Sukhwinder Singh Sran, Lakhwinder Kaur, Gurjeet Kaur, Sukhpreet Kaur Sidhu, "Energy Aware Chain Based Data Aggregation Scheme for Wireless Sensor Network", IEEE, 2015.
[17] V.Akila, Dr.T.Sheela, "Secure Data Aggregation to Preserve Data and Key Privacy in Wireless Sensor Networks with Multiple Sinks", IEEE, 2019.
[18] Jinhuan Zhang, Peng Hu, Fang Xie, Jun Long, and An He, "An Energy Efficient and Reliable In-Network Data Aggregation Scheme for WSN", IEEE Access, 2018.
[19] M. Bennani Mohamed Taj, M. AIT KBIR, "ICH-LEACH: An enhanced LEACH protocol for Wireless Sensor Network", IEEE, 2016.
[20] Surinder Singh, Hardeep Singh Saini, "Security approaches for data aggregation in Wireless Sensor Networks against Sybil Attack", IEEE, 2018.
[21] Haythem Hayouni, Mohamed Hamdi, "Secure Data Aggregation with Homomorphic Primitives in Wireless Sensor Networks: A Critical Survey and Open Research Issues", IEEE, 2016.
[22] P. Raghu Vamsi and Krishna Kant, "Secure Data Aggregation and Intrusion Detection in Wireless Sensor Networks", IEEE, 2015.
[23] Xiang Yang, Dengteng Deng, Meifeng Liu, "An Overview of Routing Protocols on Wireless Sensor Network", IEEE, 2015.
[24] H.S.Annapurna, M.Siddappa, "Secure Data Aggregation with Fault Tolerance for Wireless Sensor Networks", IEEE, 2015.
[25] R Menaka, R Dhanagopal, N Archana, "An Efficient Approach for Secured Data Aggregation Against Security Attacks in WSN", IEEE, 2020.
[26] Dnyaneshwar S Mantri, Neeli Rashmi Prasad, Ramjee Prasad, "Synchronized Data Aggregation for Wireless Sensor Network", IEEE, 2014.
[27] Opeyemi A. Osanaiye, Attahiru S. Alfa, And Gerhard P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks", IEEE Access, 2017.
[28] Ali Ghaffari, "An Energy Efficient Routing Protocol for Wireless Sensor Networks using A-star Algorithm".
[29] Sk Md Mizanur Rahman, Mohammad Anwar Hossain, Maqsood Mahmud, Muhammad Imran Chaudry, Ahmad Almogren, Mohammed Alnuem, Atif Alamri, "A lightweight Secure Data Aggregation Technique for Wireless Sensor Network", IEEE, 2014.
[30] Jia Xibei,Zhang Huazhong, Zhang Jingchen, "Research of Data Aggregation Routing Protocol in WSN Data-Related Applications", IEEE, 2010.
[31] Scott A. Thompson Jr. and Bharath K. Samanthula, "Optimized Secure Data Aggregation in Wireless Sensor Networks", IEEE, 2017.
[32] Rakesh Kumar Ranjan, S. P. Karmore, "BIST Based Secure Data Aggregation in Wireless Sensor Network", IJSR, 2013.
[33] Sukhchandan Randhawa, Sushma Jain, "Data Aggregation in Wireless Sensor Networks: Previous Research, Current Status and Future Directions", Springer, 2017
[34] V.Selvi, Dr.R.Umarani, "Comparative Analysis of Ant Colony and Particle Swarm Optimization Techniques", International Journal of Computer Applications, 2010.