Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

K-medoid based Efficient and Sustainable Utilizations of Sensor Networks with Minimal Traffic

Chopparapu Gowthami[1], Abdullah Albalawi[2], Shankar Prasad Mitra[3], Sonu Rana[4], Dhanashri Dhananjay Bhosrekar[5], Bechoo Lal[6*]

[1,6]Department of CSE, Koneru Lakshmaiah Education Foundation (KLEF), KL University Vijayawada Campus, Green Fields, Vaddeswaram, Andhra Pradesh 522302, India
[2]Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia.
[3,4]Deperment of Computer Science and Engineering, Brainware University, Barasat, Kolkata, West Bengal, Pin 700125, India
[2]Greenfingers College of Computer & Technology, Yashwant nagar, Akluj 413118, Sholapur, Maharashtra, India
Authors Email: chgowthami@kluniversity.in[1], aalbalawi@su.edu.sa[2] ,spm.cse@brainwareuniversity.ac.in[3], srn.cse@brainwareuniversity.ac.in[4], dhanashri188@gmail.com[5], bechoolal@kluniversity.in[6]*

ARTICLEINFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

Introduction: This research study introduced the Efficient and Sustainable Utilizations of Sensor Networks with Minimal Traffic during the wireless network transmission. The components are interlinked and function in a collaborative manner to transmit accumulated data to a central sink or base station that receives it. Efficient and sustainable utilization 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.

Objectives: The objective is to enhance data collection in wireless sensor networks, to identify the Efficient and Sustainable Utilizations of Sensor Networks with Minimal Traffic, thereby demonstrating an improved cluster head selection rate and a better minimum distance rate between two nearby nodes through the proposed scheme.

Methods: 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.

Results: 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.

Conclusions: The researcher proposed 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.

Keywords: WSN, DD, SPIN, SAR. Particle Swarm Optimization (PSO), k-medoid.

INTRODUCTION

The utilization 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 [1]. 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 [2]. This gives rise to several security concerns [3].

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 [4].

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[5].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 1.1. 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 [6].

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 [[7]].

The network in question is unmonitored and lacks hardware that is resistant to tampering, owing to its significant features and wireless setting [8]. 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 [9].

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 [10].

In this technique utilised to enhance network longevity through the consolidation of data, utilizing metrics such as minimum, maximum, and average values to optimize energy consumption. 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 [11].

Lein Harn et.al.,(2021) Summary: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[12]. 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. 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[13].

Cong Peng et.al.,(2021) Summary: The 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[14]. 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. This approach aims to achieve a harmonious equilibrium between data accessibility and confidentiality. Initially, a Chinese the rest theorem conversion technique is devised, incorporating a counter to encode information with multiple dimensions into large integers[15].

Gul Sahar, et.al.,(2021) Summary: Wireless networked sensors (WSNs) are widely recognized as generators of substantial volumes of data that are highly informative. The categorization of data- in Wireless Sensor Networks (WSNs) comprises four types, namely query-driven, driven by events. The implementation of targeted data in real-time applications. Numerous obstacles arise during the process of data collection[16]. Hence, the primary aim of employing models driven by data is to conserve the energy of Wireless Sensor Networks (WSNs) while facilitating the data collection process for various applications. This article provides a comprehensive overview of the latest developments in data-driven models as well as application types forWSNs[17].

OBJECTIVES

The objectives of the research study on “Efficient and Sustainable Utilizations of Sensor Networks with Minimal Traffic Using Object Orient Design” are to identify the efficient and sustainable utilization of sensors network with minimum network traffic[18] . A sensor network that is wireless is made up of several crucial components, including sensors, base stations, and users. Pressure, temperature, sound, and other non-electrical characteristics may all be measured by a sensor, and the sensor can then broadcast this data to the base station via an internal transceiver[19][20]. Given that the sent data may include crucial information, security of such data is crucial. The prioritization of wireless sensor security for networks has emerged as a significant concern, given its extensive applications in both military and public domains[21].

METHODS

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[22]. 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 [23].

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[24]. 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 [26].

The concept of energy efficiency refers to the ability to achieve a desired level of energy output while minimizing energy input[27]t. 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[28]. However, in practical situations. The energy is 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[27].

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

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[28].

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

NL_n^n= Life Time of Network

NL_v= Life Time of V Node

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[29]. 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. [30].

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[31].

In the domain of Wireless Sensor Networks (WSNs), the transfer of data from the sensor nodes to sink the nodes is facilitated through the utilization of data-driven models that have been tailored to accommodate the inherent features of the information being transmitted[32]. The utilization of models based on data is prevalent in the field of Wireless Sensor Networks (WSNs) for the purpose of analyzing specific objects of interest. The objects mentioned above are categorized into four main data-driven models, as depicted in Figure. Several models have been put forth in the scholarly literature, such as the query-driven approach, driven by events model, time-dependent model, continuous-driven approach, and hybrid-driven models [33].

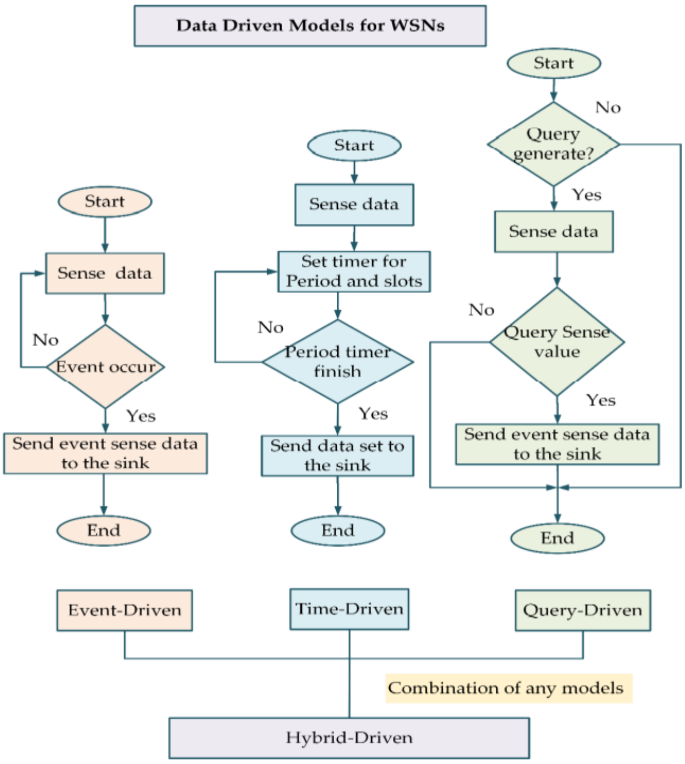


Figure1. Process of data-driven models for WSNs [6]

The data analyzing methodologies utilized by everyone data-driven model demonstrate variations[34]. 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[35]. 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 [34].

The path-based detection algorithm is characterized by a node's observation of its immediate neighbour to the current route path, rather than monitoring all nodes in the neighbourhood. 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 neighbouring 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 neighbour to be a black hole and abstains from transmitting packets to the suspected nodes in subsequent occurrences [35].

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

1. The Exponential Trust-based mechanism involves the maintenance of a streak opposite (n) to monitor the consecutive dropping of packets.Theutilisation 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.
2. The trust factor experiences an exponential decrease as a packet is dropped.
3. 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 [35] is determined based on the provided information.

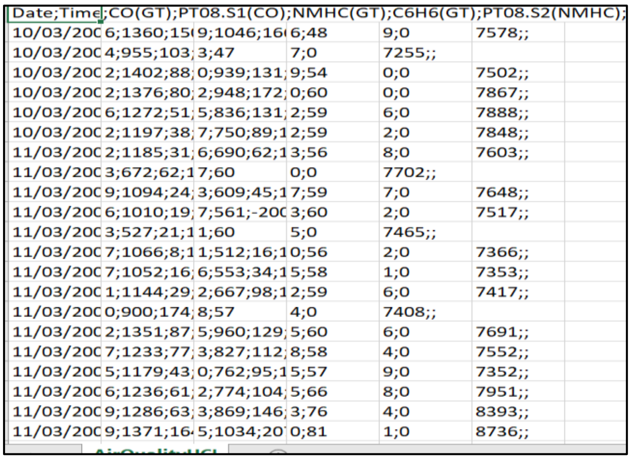
$$Reliability\ Ratio = \frac{No.\ of\ packet\ sent}{No.of\ packets\ Received} ....(3)$$

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.

RESULTS

The implementation of firewall as well as router filtering techniques is crucial in ensuring network security. A firewall refers to a network device, such as a network router or a computer, which actively monitors the flow of packets and safeguards the system against unauthorized and potentially harmful access. Firewalls have the capability to function as a relay or a semi-transparent gateway in order to mitigate Denial of Service (DoS) attacks.

A firewall may be conceived as a partially transparent gateway. The transmission of a SYN packet to a host is initiated by the firewall, eliciting a subsequent response from the host in the form of a SYN+ACK packet. In the context of legitimate connections, the TCP protocol discards duplicate ACKs received by the host, allowing subsequent packets to flow unhindered by the firewall. This approach ensures that there are no delays imposed on legitimate connections.



Date;Time	;CO(GT);PT08.S1(CO);NMHC(GT);C6H6(GT);PT08.S2(NMHC);				
10/03/200	6;1360;15	9;1046;16	6;48	9;0	7578;;
10/03/200	4;955;103;	3;47	7;0	7255;;	
10/03/200	2;1402;88;	0;939;131;	9;54	0;0	7502;;
10/03/200	2;1376;80;	2;948;172;	0;60	0;0	7867;;
10/03/200	6;1272;51;	5;836;131;	2;59	6;0	7888;;
10/03/200	2;1197;38;	7;750;89;1	2;59	2;0	7848;;
11/03/200	2;1185;31;	6;690;62;1	3;56	8;0	7603;;
11/03/200	3;672;62;1	7;60	0;0	7702;;	
11/03/200	9;1094;24;	3;609;45;1	7;59	7;0	7648;;
11/03/200	6;1010;19;	7;561;-200	3;60	2;0	7517;;
11/03/200	3;527;21;1	1;60	5;0	7465;;	
11/03/200	7;1066;8;1	1;512;16;1	0;56	2;0	7366;;
11/03/200	7;1052;16;	6;553;34;1	5;58	1;0	7353;;
11/03/200	1;1144;29;	2;667;98;1	2;59	6;0	7417;;
11/03/200	0;900;174;	8;57	4;0	7408;;	
11/03/200	2;1351;87;	5;960;129;	5;60	6;0	7691;;
11/03/200	7;1233;77;	3;827;112;	8;58	4;0	7552;;
11/03/200	5;1179;43;	0;762;95;1	5;57	9;0	7352;;
11/03/200	6;1236;61;	2;774;104;	5;66	8;0	7951;;
11/03/200	9;1286;63;	3;869;146;	3;76	4;0	8393;;
11/03/200	9;1371;16	5;1034;20	0;81	1;0	8736;;

Figure 1. Dataset

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

Table 1. Network Parameters

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

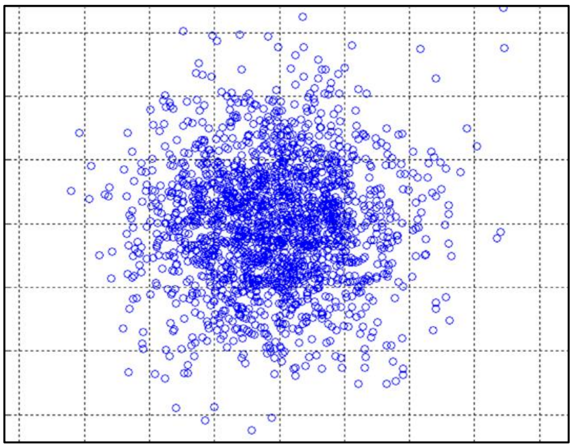


Figure 2.K-medoid clustering

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.

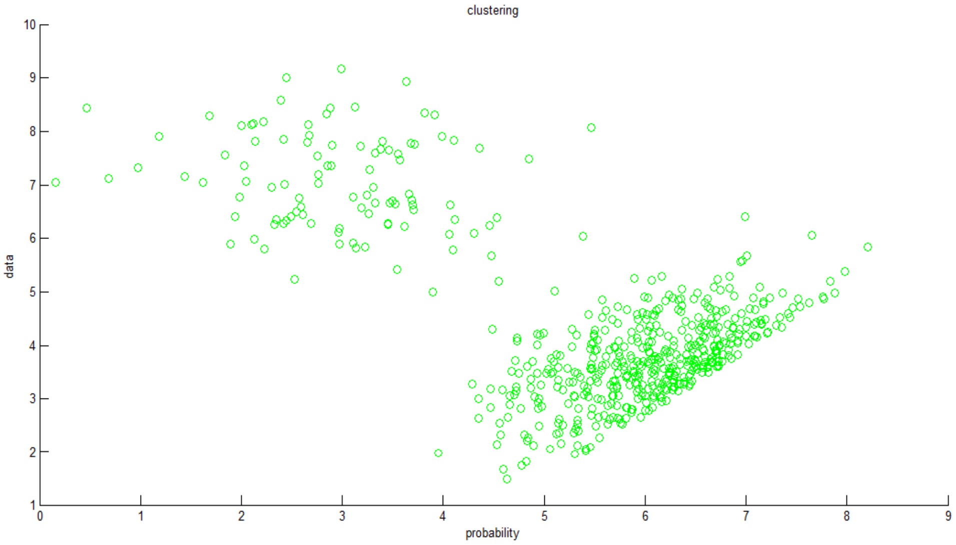


Figure 3. Clustering

Apply clustering mechanism and based on grouping and probability-based estimation create group of clusters. 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 collections not only contribute to energy conservation, but also eliminate 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 neighbouring 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.

DISCUSSION

Finally the researcher concluded that the proposed research study on energy-efficient coverage control algorithm for WSNs based on Particle Swarm Optimization (PSO) – K Medoid is more significant to optimize the minimum traffic during wireless network transmission .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. This research study presents a novel approach for achieving energy efficiency in the process of data aggregation within wireless sensor networks. Our proposed scheme incorporates mechanisms that aim to optimise energy efficiency and enhance data storage capabilities Wireless Sensors Networks (WSNs).

REFRENCES

[1] Supriya H.S, Dr. Dayananda R.B, “Nearest Neighbor Monitoring Mechanism for Efficient and Secur e 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”, IE EE, 2020.

[4] Lein Harn, ChingFang 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 DataDriven Models in Wireless Sensor Networks: A Survey”, MDPI, 2 021.

[7] Dr. Akella Amarendra Babu, Dr. G. Dileep Kumar, Dr. R. BalaMurali, Dr. K. Kondaiah, “Wireless Sensor Networks: Data Aggregation Using LEACH Routing Protocol”, NCACNM, 2017.

[8] Naveen Kumar, Jyoti R. Desai, Dr. Annapurna D, “ACHsLEACH: 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 Techni ques 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, Asso. Prof., Dr.K.Chitra, Professor, C.Selvakumar, Professor, “Energy Efficient Clu stering In Wireless Sensor Networks”, IEEE, 2017.

[13] V.Akila, Dr.T.Sheela, “Preserving Data and Key Privacy in Data Aggregation for Wireless Sensor Ne tworks”, IEEE, 2017.

[14] Aishah Aseeri, Rui Zhang, “Secure Data Aggregation in Wireless Sensor Networks: Enumeration Att ack 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, "ICHLEACH: 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.

[35] Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani, "Routing Attacks in Wireless Sensor Networks: A Survey".