Advances in Dynamical Systems and Applications (ADSA).
ISSN 0973-5321, Volume 16, Number 2, (2021) pp. 683-701

https://www.ripublication.com/adsa.htm

Optimal Cluster-Based Data Aggregation in WSN for Healthcare Application

Sree Ranjani N Y[1], Dr. A G Ananth[2], Dr. L Sudershan Reddy[3]

[1]Research Scholar, Department of Electronics and Communication Engineering, JAIN (Deemed-to-be University), Bangalore, India

[2]Professor, Department of Electronics, NMAM Institute of Technology, Mangalore, India,

[3]Professor, Department of Management Studies, JAIN (Deemed-to-be University), Bangalore, India,

Abstract

Healthcare is one of the most important and rapidly growing application areas for WSNs. This is driven by the motivation to improve the healthcare industry's accuracy and efficiency. The WSN brings a number of significant improvements to healthcare, but, as it is deployed in an exposed environment, it is the weakest link that needs the most protection. Due to limitations in communication such as power, storage and the computational capabilities of sensors, data aggregation techniques are used to reduce the communication overhead in real-time data transmission, maximizing the network lifetime, energy conservation measures are essential for improving the performance of WSNs. In this paper energy consumption issue by designing systems optimal cluster-based data aggregation is proposed. Data aggregation is an effectual approach for wireless sensor networks (WSNs) to save energy and prolong network lifetime. Also, Cluster-based data aggregation algorithms are most popular because they have the advantages of high flexibility and reliability. The efficient clustering is performing by the glow-worm swarm optimization. After clustering it is important to select the CH among multiple nodes in the cluster, which act as data aggregation node. The experimental results are analyzed with existing algorithms to show the proposed system OCDA is more effective compared to SPPDA system.

Keywords: Cluster Head, Data aggregation, Wireless Sensor Network, Glowworm Swarm Optimization, Healthcare.

1. INTRODUCTION

Wireless Sensor Network (WSN) is a self-design system of small sensor hubs, where the sensor hubs can communicate among themselves utilizing radio signals, and these sensor nodes can detect, monitor and understand the physical environment [1]. Sensor networks are primarily designed for real-time collection and analysis of low-level data in hostile environments. For this reason, they are well suited to a substantial amount of monitoring and surveillance applications [2]. WSN is always deployed in unsecured and untrusted environment, which makes it exposed to all kinds of intrusions, and encounters some serious security issue [3]. Moreover, a large number of data transmissions cause data collisions and data congestion. All these lead to the turning up of data aggregation technique [4-6].

Data aggregation is defined as the process of aggregating data from multiple sensor nodes to eliminate redundant transmission and provide fused information to a sink node. In data aggregation, there are mainly three kinds of aggregation ways. The first is clustering data aggregation where data are collected and aggregated at a cluster node and then transmitted to a sink node. The second is hop by hop aggregation, which means that data are aggregated at each intermediate node. The third is partial aggregation, where data aggregation satisfies a time or energy threshold [7]. All these three kinds of data aggregations have their drawbacks. In clustering data aggregation, a cluster head always consumes much energy than others; WSNs always perform a cluster head (CH) select algorithm to decide a new cluster head, which wastes considerable time and energy [8].

Over this interval, the sensors would continuously record signals correlated with your key physiological parameters and relay the resulting data to a database linked with your health records. Using the available data, and aided by decision support systems that also have access to a large corpus of observation data for other individuals, the doctor can make a much better prognosis for your health and recommend treatment, early intervention, and life-style choices that are particularly effective in improving the quality of your health [9-12].

The remaining parts of this paper is organized as follows. In section 2, the literatures on existing methods are reviewed. Section 3 describes the problem statement. The proposed methodology is detailed in section 4. Results and discussion of proposed and existing methods are discussed in section 5. The overall conclusion of this paper is provided at section 6. The objective of this work is to propose optimal cluster-based data aggregation (OCDA) technique by optimizing the waiting time at nodes in order to obtain a tradeoff between energy and delay for healthcare application.

2. LITERATURE REVIEW

Selvakumar and Sankaranarayanan [13] have developed a routing algorithm called cluster-chain mobile agent routing (CCMAR). The presented method makes full use of the advantages of both low energy adaptive clustering hierarchy (LEACH) and power-efficient gathering in sensor information systems (PEGASIS). CCMAR divides the WSN into a few clusters and runs in two phases. In phase 1, all the nodes

in each cluster form a chain to perform data aggregation within the clusters. In phase 2, a MA was dispatched from the sink node to collect the aggregated data from all cluster/chain head nodes. It was inferred that the performance of the data aggregation using routing protocol was strongly influenced by the underlying network topology. However the network topology used here is complicated by which it consumes more energy, so that the life time will be very low.

Anees Ara and et. al [14] have proposed SPPDA method that utilizes the homomorphic property of the Bilinear ElGamal cryptosystem to perform privacy-preserving secure computation and combines it with the aggregate signature scheme, enabling data authenticity/integrity in the WBAN. The SPPDA scheme have shown semantically secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Security analysis demonstrates that the method preserves data confidentiality, data authenticity, and data privacy; it also resists passive eavesdropping and replay attacks. In spite of all those security analysis the energy efficiency of the system is not mentioned here in this SSPDA method, this may be considered as a major limitation.

Ramnik and Anil [15] have presented the networks which are heterogeneous and are based on the adaptive threshold sensitive distributed energy efficient cross layer routing protocol. The concept of weighted probability was used to assign the CH (Cluster Head) of the network cluster. The basic advancement of hybrid technique ATEER was the consideration of all the three levels of node heterogeneity. The CHs have been selected in accordance to the ratio calculated from the average energy of entire network and residual energy of the sensor node. However the lifetime of the network is not considered here in this paper, also the power consumption is very high.

Suneet K. Gupta and Prasanta K. Jana [16] have presented genetic algorithm-based approaches for clustering and routing in wireless sensor networks. The clustering was based on residual energy of the gateways and distance from sensor nodes to their corresponding cluster head. The routing scheme was also based on the residual energy of the gateways along with a trade-off between transmission distance and number of forwards. They have shown that the clustering algorithm balances the lifetime of the gateways as well as reduces the energy consumption of the sensor nodes. The routing algorithm has been developed by considering a trade-off between transmission distance and the number of hop-count. Anyhow the lifetime of the network is not demonstrated here in this paper.

Harmanjeet and et. al [17] have proposed PPCF scheme based on multi-party random masking and polynomial aggregation techniques. Two phases have been considered: off-line model generation and online prediction generation. Three protocols have been considered for privacy preservation and analysis of each protocol is done separately. The Paillier homomorphic encryption system is used to calculate the length of vector X securely, and only additive property of homomorphic encryption is used. Analysis of the method have been done for security, accuracy, coverage and performance on healthcare and Movieslens datasets. However the energy efficiency of these techniques and the lifetime of the network is explained here.

3. PROBLEM STATEMENT

Physiological states of patients are closely checked by deploying Remote sensors These sensors are utilized to detect the patient's fundamental body parameters and transmit the detected information in a convenient manner to some remote area without human contribution. Utilizing these medicinal sensor readings, the specialist can get the points of interest of a patient's wellbeing status. Number of research groups and projects have begun to develop health monitoring utilizing wireless sensor networks. Remote Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new innovations in health services applications without considering security often makes patients privacy protection vulnerable. Hence in this health monitoring application the data aggregation reduces the communication cost in the sensor network.

Any aggregator node has to carry out some more additional work than any regular node. It has to collect data from a few regular nodes, perform the aggregation by combining the collected data, maintain the routing information to reach the sink node and forward the aggregated data to the sink node. Whenever the aggregation process happens in the aggregator node, it consumes more energy than the regular node. So, the selection of an aggregator node is the typical issue. Even if an ideal node from a group is chosen as an aggregator node and if the same node is acting as an aggregator for a long time, then it will be overloaded and wit will lose more energy soon. Hence not only the aggregator selection, the aggregator maintenance is also a major issue. The figure 1 shows the system architecture of healthcare application in WSN.

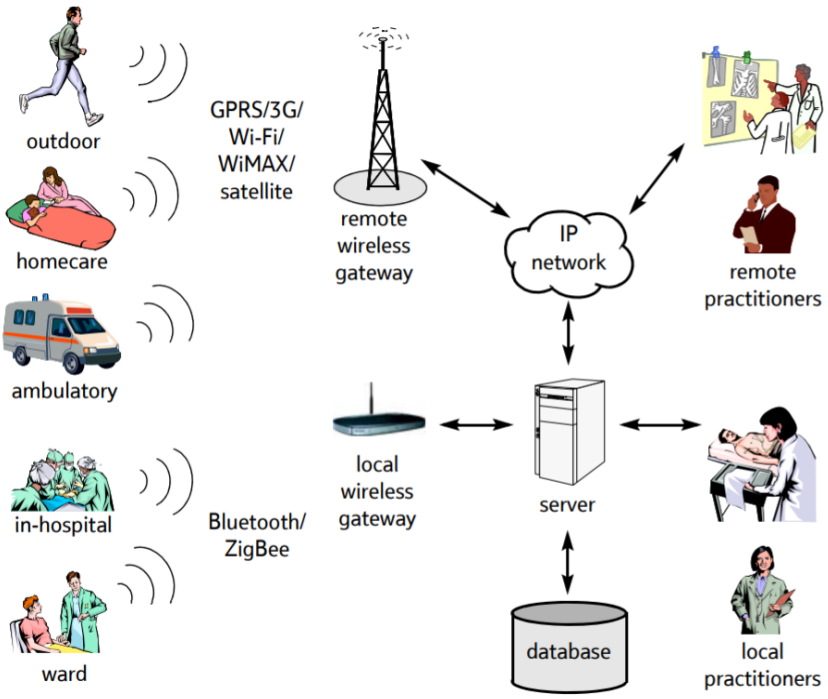

Figure 1: System Architecture of WSN in Healthcare Application

The primary security objective of the proposed scheme is to maintain the confidentiality of data been transmitted by the sensors to the remote server. The goal is also to retain the integrity of the data, which can be achieved by authentication of the data source. Additionally, the proposed scheme should maintain the medical data anonymity/data privacy without allowing any adversary to identify the content of the data. Finally, the freshness of data has to be maintained to know the exact current status of the patient for timely diagnosis and treatment.

4. PROPOSED OPTIMAL CLUSTER-BASED DATA AGGREGATION MODEL

In this system, it focuses on collection and transmission of the patient's privacy-preserving health data to the server. Specifically, this process can be done in three stages such as secure optimal cluster-based data aggregation, secure data transmission and Maintenance/Accessing stage. Initially Glow swarm optimization Algorithm is used for clustering process. During clustering some nodes are residual not become part of any cluster. These Residual nodes are prevented using GSO with fitness calculation between nodes. After clustering, CH is selected which acts as the aggregator node, where each CH make use of CHs as a forwarding node to base station as a result the transmission energy is reduced. Also, the cluster members are needed to be in active state only for its TDMA slot thus for the remaining time they are in sleep state so this proposed research increases the lifetime of the network that helps to the improve the performance of application. The system model is shown in figure 2.

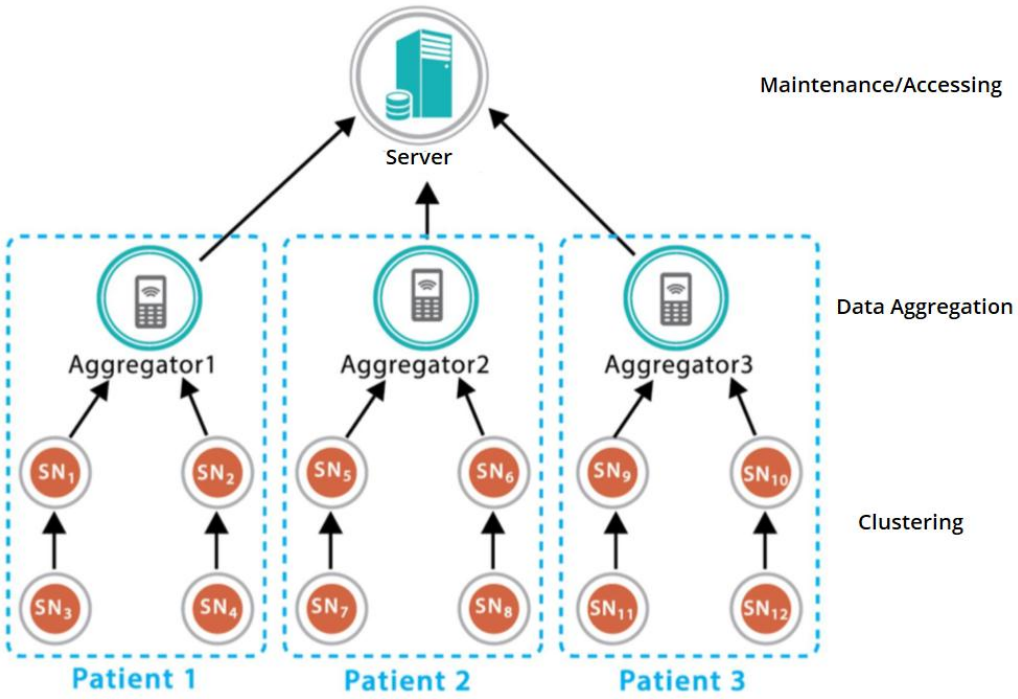

Figure 2: System Model

4.1 Health Monitoring process

At first, the patient's data has been applied to the data aggregator using the following sensors such as blood pressure, pulse oximetry, ECG, and motion is represented as sensing nodes. Then the data aggregator collects all the health information for the analysis of those data and aggregate each user's health data and report the aggregated data to the remote medical server honestly, but it is also curious about the individual sensor's readings.

4.2 Confidentiality and Data Privacy

To protect the patients' sensitive health data, which was collected from the sensors, it cannot identify the contents of the data packet. Also, if the adversary tries to have unauthorized access to the database, it cannot identify the individual sensor's data. In this way, sensor's data can achieve the privacy-preserving requirement. Confidentiality also includes the prevention of aggregated data being identified by any adversary, except the authorized MS.

4.3 Authentication and Data Integrity

To authenticate encrypted health data that has been collected and sent by a legitimate medical sensor and not altered during transmission i.e., if an adversary forges and/or modifies a report, malicious operations should be detected so that proper data aggregation is done and correct health data is received at the server.

The primary security objective of this proposed scheme is to maintain the confidentiality of data been transmitted by the medical sensors to the remote server. The goal is also to retain the integrity of the data, which can be achieved by authentication of the data source. Additionally, the proposed scheme should maintain the medical data anonymity/data privacy without allowing any adversary to identify the content of the data. Finally, the freshness of data has to be maintained to know the exact current status of the patient for timely diagnosis and treatment. Hence to achieve this effective and optimal cluster-based data aggregation has to be processed and are as follows:

4.4 Optimal cluster-based data aggregation

Cluster based data aggregation is the common solution for energy efficient data transmission in wireless sensor networks. The figure 3 shows the optimal cluster-based data aggregation.

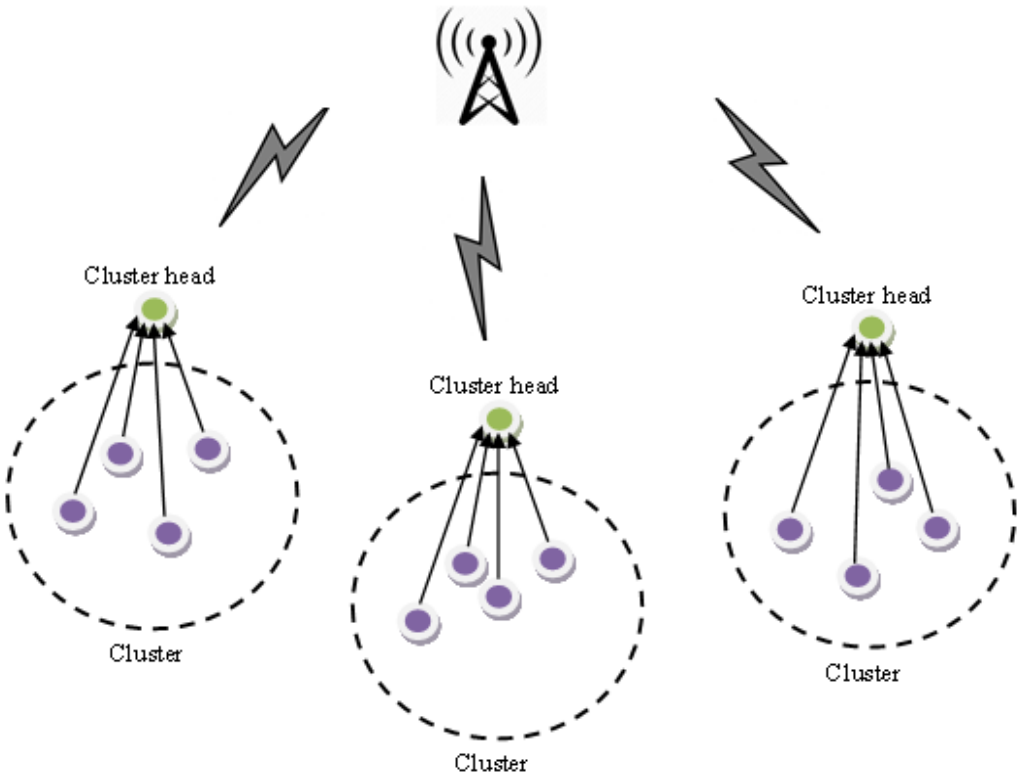

Figure 3: Optimal cluster-based Data Aggregation

Cluster Formation phase

In this phase, whole network is separated into C layers. Then each layer is divided into a set of clusters. BS initiates this phase. In the network region NR, ω is the distance of a node which is far away from the BS in the region NR.

$$\omega = \max\left(\nabla_{j=1}^{M} e\left(se_j, BS\right)\right) \quad \text{---------- (1)}$$

Where $e\left(BS, se_j\right)$ is distance between the BS and the sensor node se_i. To provide the communication between the CHs in two adjacent layers BS uses the minimum radio transmission range to split the network into layers. Number of layers C depends upon this ω and the minimum radio transmission range, $TRANS_{r-\min}$ of the sensor node.

$$C = \frac{\omega}{TRANS_{r-\min}} \quad \text{----------(2)}$$

Let $l = \left\lfloor \frac{e\left(se_j, BS\right)}{TRANS_{r-\min}} \right\rfloor ; se_j \in l^{th} layer$; where $1 \geq l \leq C$ ----------(3)

The node with lesser distance belongs to the closer layer. One hop distance node belongs to first layer, two hop distance node belongs to second layer and l hop distance node belongs to l^{th} layer. Here the hop distance is based on the minimum transmission rang of the node. As a result, all M nodes fit into any one of the C layers. Now each layer l is further divided into K clusters. Since all the CH reach the BS via the intermediate CHs, the CHs closer to the BS drain their energy soon. To reduce this trouble, the K value is to be assigned cautiously. The layers which are closer to the BS have larger K, i.e. $K1 > K2 > K3 \ldots > KC$. Number of clusters K is directly proportional to the layer number. That is, if a layer is having huge number of nodes then that layer should have good number of clusters. Layer with the smaller layer number should have the greater K and with the greater layer number should have the smaller K. According to these facts the number of clusters K for the layer l is defined as:

$$Kl = \frac{n(l)}{(l \times C)} \quad \text{----------} \quad (4)$$

Where $n(l)$ is the number of nodes in layer l. In each layer l, Kl number of clusters is formed by using the K-means algorithm. K-means clustering generates a specific number of disjoint, flat clusters. As a final point, this phase forms Kl clusters in all layers. This cluster formation is carried out only once in the network thus optimal cluster-based data aggregation reduces some amount of message transmission and it can increase the lifetime of network. But in the maintenance phase cluster setup is altered if the cluster has too small number of alive nodes. Once the clusters are finalized, optimal cluster-based data aggregation elect an optimum node as a cluster head. The efficient clustering is performed by the behavior of glow-worm swarm optimization.

4.5 Glowworm Swarm Optimization Algorithm

Glowworm swarm optimization (GSO) algorithm is one of the newest nature inspired heuristics algorithms for optimization problem. GSO algorithm is proposed for the simultaneous computation of multiple optima of multimodal functions. In the GSO algorithm, a swarm of agents (particles or glowworms) is initially deployed randomly in the solution space. These agents are modeled based on glowworms, which belong to a family of beetles. This glowworm emits bioluminescent light to attract its mates or prey. The brighter the glow, the more is the attraction. The glowworm emits light, whose intensity is proportional to the associated luciferin value and it interacts with other glowworms within a variable neighborhood. This glowworm characteristic is imitated in the GSO algorithm to find the multiple optimal points in the solution space. Accordingly, the agents carry a luminescence quantity called luciferin along with them. Each agent selects a neighbor that has a luciferin value more than its own (within the local decision range) and moves towards it using a probabilistic mechanism.

Phase 1: Luciferin update phase

Even though all the glowworms start with equal luciferin values, these values change according to each glowworm fitness value at their current position. In case of optimization problem, this luciferin value changes based on the problem's overall fitness value. The luciferin update rule is described with the following equation:

$$l_i(s+1) = \max\{0, (1-\rho) l_i(s) + \gamma K_i(s+1)\} \quad \text{---------- (5)}$$

Where ρ is the luciferin decay constant $(0 < \rho < 1)$; γ is the luciferin enhancement constant, $l_i(s)$ represents the luciferin value associated with i^{th} glowworm at time s and $K_i(s)$ represents the problem objective function value of the i^{th} glowworm at time *s*.

Phase 2: Movement phase

As a first step in the movement phase, each glowworm identifies a set of neighbors using the rule given in the following equation:

$$M_j(s) = \{i : e_{ji}(s) < q_e^j(s); l_j(s) < l_i(s)\} \quad \text{---------- (6)}$$

Where $M_j(s)$ represents a set of neighbors' for the j^{th} glowworm at time s; $e_{ji}(s)$ represents the Euclidian distance between the j^{th} and i^{th} glowworm at time s; $q_e^j(s)$ represents the local decision range value of the i^{th} glowworm at time s, which is bounded by radial sensor range $q_t (0 < q_e^j < q_t)$.

In the second step of movement phase, probabilistic mechanism is used to identify a unique neighbor from the set of neighbors. For every glowworm j, the probability with respect to its i^{th} neighbor is calculated using the following equation:

$$U_{ji}(s) = \frac{(l_i(s) - l_j(s))}{\sum_{G \in M_j(s)} (l_G(s) - l_j(s))}, \quad where\ i \in M_j(s) \quad \text{---------- (7)}$$

Where $U_{ji}(s)$ is the probability of moving the j^{th} glowworm towards the i^{th} neighbor at time s. As a third step in the movement phase, each glowworm j identifies i^{th} glowworm as its unique neighbor with maximum probability value as a selection criterion and it is calculated using the above equation. Now as a core part of

movement phase, each glowworm moves towards its own unique neighbor using the following equation:

$$y_j(s+1) = y_j(s) + T\left(\frac{(y_i(s) - y_j(s))}{\|y_i(s) - y_j(s)\|}\right) \quad \text{---------- (8)}$$

Where $y_j(s)$ is the location of glowworm j at time s, $\|\ \|$ is the Euclidean norm operator and T is the step size which changes according to the below equation, as given below:

$$T = T^{\max} - \left(\frac{\left(T^{\max} - T^{\min}\right)}{Maximum\ no\ of\ iterations}\right) \times iteration \quad \text{---------- (9)}$$

Where $T^{\max}$ and $T^{\min}$ are the boundaries for the step size T.

Phase 3: Neighborhood range update phase (or) Local decision range update phase

The neighborhood range of each glowworm is adaptively updated using the following equation:

$$q_e^j(s+1) = \min\left\{q_t, \max\left\{0, q_e^j(s) + \beta\left(m_s - \left|M_j(s)\right|\right)\right\}\right\} \quad \text{---------- (10)}$$

Where $q_e^j(s)$ is the neighborhood range (or) local decision range of the j^{th} glowworm at time s; q_t is the luciferin sensor radial range; β is a constant parameter; m_s is the neighborhood threshold; $\left|M_j(s)\right|$ is the number of neighbors in the neighborhood set of the j^{th} glowworm at time s.

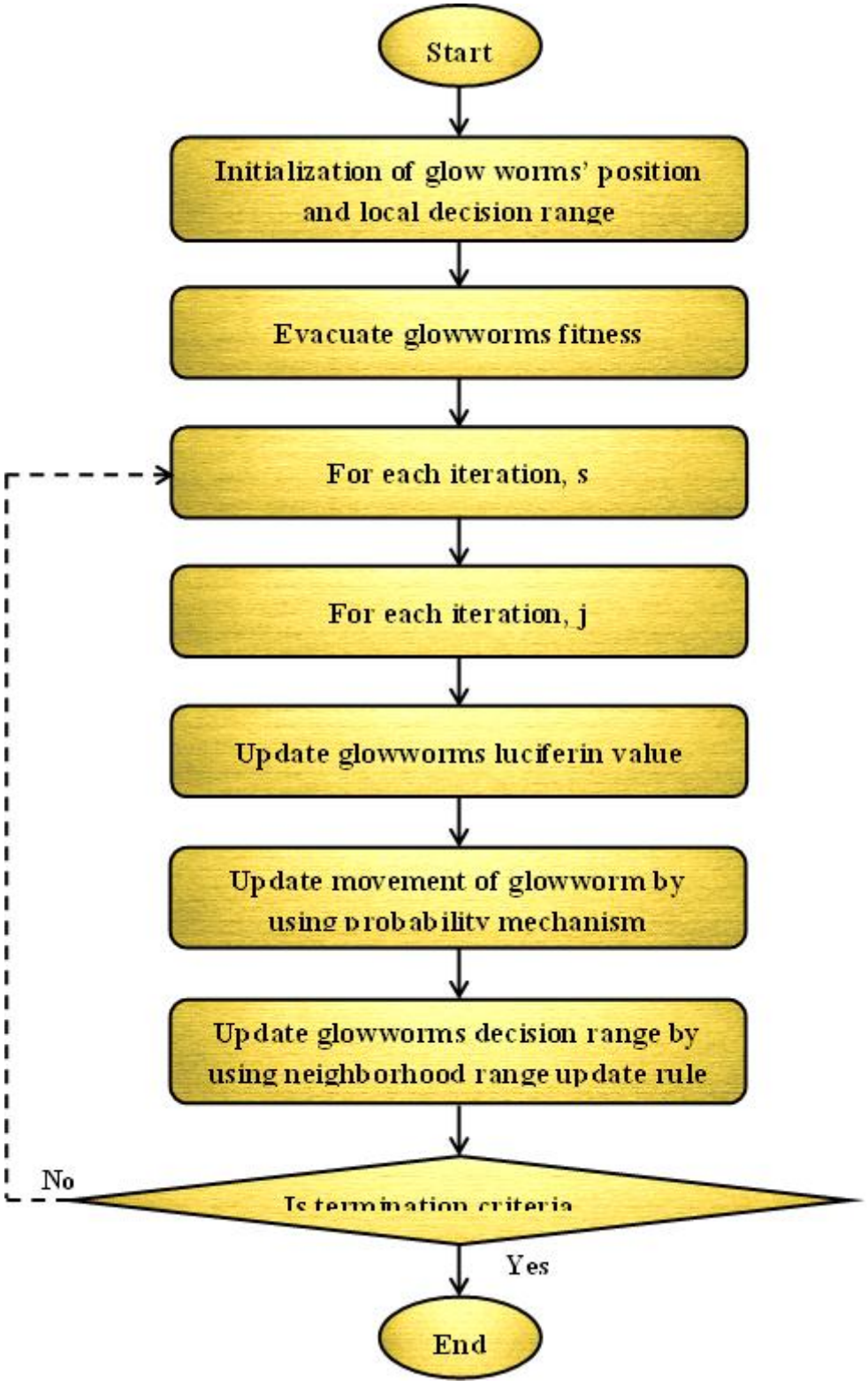

Figure 4: Flow Diagram of Glow Swarm Optimization Algorithm

4.6 Privacy Preserving Data aggregation phase

Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission. In this method the CH work as an aggregating node. By receiving the TDMA slot, all cluster members sends the monitored information to its CH. Each CH waits for one TDMA frame to collect the information from its member nodes. After each TDMA frame, CH aggregates the received information and forwards the aggregated data to the base station. In general, CHs directly transfer the data to the base station node. Energy for the direct transmission is high. But in this proposed optimal cluster-based data aggregation method, each CH make use of CHs as a forwarding node to base station as a result the transmission energy is reduced.

Cluster head is chosen based on the node's residual energy (RE_r) and the energy to communicate (CE_c) with other nodes in the cluster and the BS. Nodes in a cluster calculate their probability to become a cluster head (P_{CH}).

$$P_{CH}(se) = 1\left[\frac{\left(\left(t_{round}/t_{tf}\right)\times\left(CE_c+\psi\right)\right)+\sum_{i=1}^{n(L)}E_{ty}\left(a_{se,nm_i}\right)}{RE_r}\right] \quad \text{---------- (11)}$$

Where, ψ is the energy to perform the data aggregation. $t_{round}$is the time period of each round. t_{tf} is the TDMA frame period. So $\left(t_{round}/t_{tf}\right)$ is the total number of times that the CH needs to do the aggregation. $\sum_{i=1}^{n(L)}E_{ty}\left(a_{se,nm_i}\right)$ is the total energy to communicate with its cluster members (nm) to transmit the TDMA slots. $n(L)$ indicates the total number of nodes in the cluster. The node's residual energy RE_r is reduced for each a bit data transmission and reception. If a node se wants to become the CH then it should have the capability to communicate with its cluster members and the next hop CH to transmit the aggregated data of the current round. If the node's RE_r is less than its CE_c value then that node cannot participate in the CH election.

$$CE_c = \left\{\begin{matrix}Energy\ to\ transmit\ a\ bits\\ of\ data\ to\ its\ next\ hop\ cluster\ head\end{matrix}\right\}+\left\{\begin{matrix}Energy\ to\ receive\ a\ bits\\ of\ data\ \ from\ its\ cluster\ members\end{matrix}\right\} \quad (12)$$

$$CE_c = E_{ty}\left(a_{se,CH_{mh}}\right)+\sum_{i=1}^{n(L)}RE_{ry}(a) \quad \text{---------- (13)}$$

From the above equations, Energy to transmit a bits of data to the next hop cluster head (CH_{mh}) is,

$$E_{ty}\left(a_{se,CH_{MH}}\right)=\left(E_{elec}\times a\right)+\left(e\left(se,CH_{mh}\right)^2\times E_{amp}\times a\right) \quad \text{---------- 14)}$$

And energy to communicate with the cluster members (nm) is,

$$E_{ty}\left(a_{se,nm}\right)=\left(E_{elec}\times a\right)+\left(e\left(se,nm\right)^2\times E_{amp}\times a\right) \quad \text{---------- (15)}$$

4.7 Security based optimal cluster-based data aggregation

For the security purpose, all CHs proposed have to perform the secure data aggregation so as to consider the energy requirements to perform the Bayesian fusion algorithm in defining the communication cost.

$$CE_c=\begin{Bmatrix}Energy\ to\ transmit\ a\ bits\\ of\ data\ to\ its\ next\ hop\\ cluster\ head\end{Bmatrix}+\begin{Bmatrix}Energy\ to\ receive\ a\ bits\\ of\ data\ from\ its\\ cluster\ members\end{Bmatrix}+\begin{Bmatrix}Energy\ to\ compute\ the\\ Trust\ probability\ for\ every\\ cluster\ member\end{Bmatrix}$$

$$CE_c=E_{ty}\left(a_{se,CH_{mh}}\right)+\sum_{i=1}^{n(L)}\left[RE_{ry}(a)+\varepsilon\right] \quad \text{---------- (16)}$$

Where, ε is the energy to compute the trust probability. Once a node is elected as a CH, it broadcasts the CH message to its cluster members, to other CHs and to BS. Hence, all cluster members send its sensed data to their CH during its allotted time slot. Cluster head nodes are calculating the total trust. So, the computation power consumptions in the low energy cluster members are avoided. Once the cluster head identifies untrustworthiness of any node inside the cluster, it immediately alerts the remaining cluster members about the malicious node in the cluster. So the cluster member discords the data from the malicious node. Security threat is identified by the highest power node, and the malicious node is detected in a small group, thus the energy consumption for detecting the untrustworthy node is reduced in this approach.

4.8 Authentication Phase

Optimal cluster-based data aggregation method evenly distributes the load for all nodes in the cluster. If the cluster head is static, its node always dissipates more energy. If the total number of nodes alive in a cluster is less than the obtained percentage of its initial number of nodes then that cluster members joins with other

closer clusters in the same layer. Also, the proposed method can further decrease the overall computational cost due to scalar multiplications by limiting the product at the aggregator to a threshold value. It can be noted that by small additional cost, a much efficient end-to-end secure privacy-preserving data aggregation method can be proposed for the remote health monitoring system

5. RESULT AND DISCUSSION

This section discusses about the performance of proposed OCDA technique by comparing existing approaches. This section also evaluates the computational complexity with respect to delay, energy aware data transmission and cost. The performance evaluation is implemented in NS2 and the results of OCDA (Optimal Clustering based Data aggregation) approach is compared with SPPDA (Secure privacy preserving Data aggregation) techniques by reducing the communication complexity, reducing computational overhead and also improving the efficiency of the proposed method.

The figure 5 shows the comparison of Network lifetime for proposed OCDA and existing SPPDA approach. Most descendant routing protocols follow the idea with attentions on the rules of cluster head selection the experimental results are shown in Fig. (5). In contrast to the results using the OCDA has a significantly larger number of alive nodes. In other words, the proposed approach ensures a longer network lifetime than the existing approach. The important security and privacy preserving measures of a health monitoring system using WSN are Data confidentiality, Data authentication, Strong user authentication, Data integrity, Access control, Data availability, Data freshness, Secure localization, Forward and backward secrecy, Patient permission, Communication and computation cost. The table 1 shows the comparison table of network lifetime for SPPDA and Proposed OCDA.

Table 1: Comparison of Network lifetime for SPPDA and Proposed OCDA

Iterations	**No. of Live Nodes**	
	SPPDA	OCDA
10	95	97
20	30	50
30	10	23
40	4	13
50	1.5	7
60	0	0.5

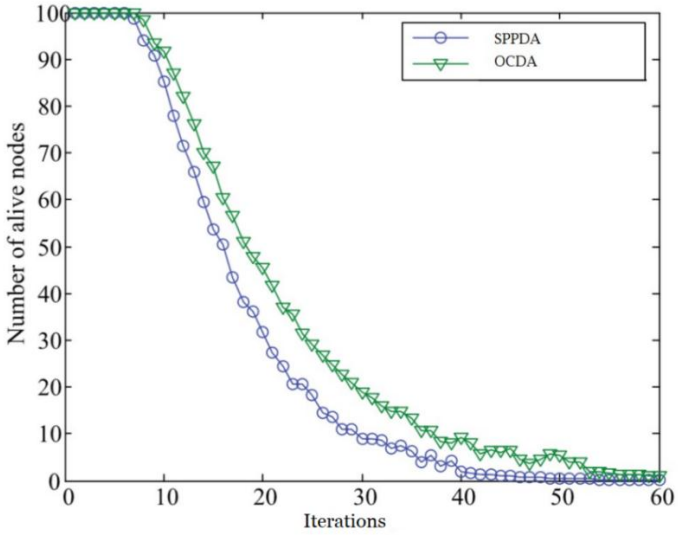

Fig 5: Comparison of Network Lifetime

The figure 6 shows the Comparison of Computational complexity at the Aggregator for OCDA and SPPDA. The computational efficiency of the proposed OCDA approach in comparison with non-aggregate approach is analyzed by varying the network scale. Hence it is very clear the OCDA approach performs better than the non-aggregate scheme. Also, it is clear that the optimal clustering-based data aggregation is used for health monitoring application. The table 2 shows the comparison of computational time for proposed OCDA and existing SPPDA.

Table 2: Comparison of Computational complexity of Proposed OCDA with Existing SPPDA

Number of sensors	**Computational Time**	
	SPPDA	OCDA
2	20	12
4	28	19
6	35	28
8	42.5	34
10	52.5	43

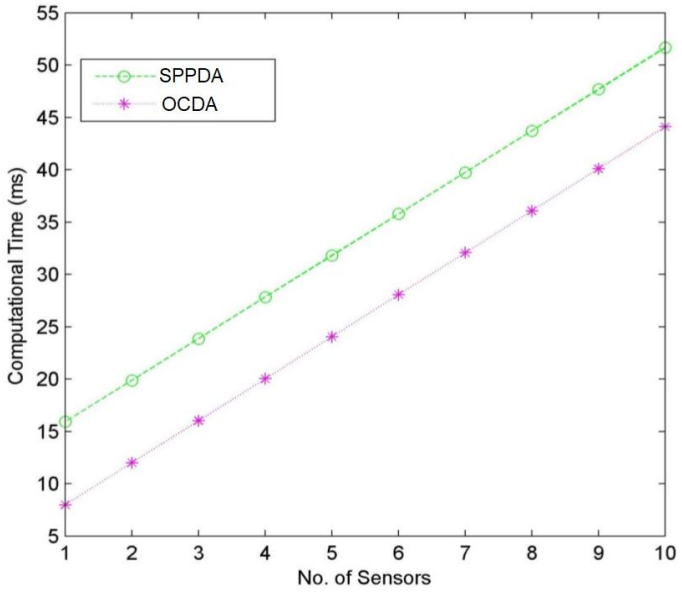

Fig 6: Comparison of Computational complexity at the Aggregator for OCDA and SPPDA

The figure 7 shows the comparison of Computational complexity at the Server with OCDA and Existing schemes. It is clearly shown from figure (7) that the proposed OCDA scheme largely reduces the computational complexity at the aggregator and also at the server. From the above analysis, the proposed OCDA scheme is indeed efficient in terms of simulation results and computational complexity, which is suitable for privacy preserving data aggregation in health monitoring systems. The table 3 shows the comparison of computational complexity at the sever for proposed OCDA and existing algorithms.

Table3: **Comparison of Computational complexity at the Server for proposed OCDA and Existing algorithms**

Number of sensors	DSROC	EDG	SPPDA	OCDA
2	12	18	12	8
4	12	17	12	8
6	11.5	23	12.1	8
8	11.5	33	12.2	8
10	11.6	40	12.5	8

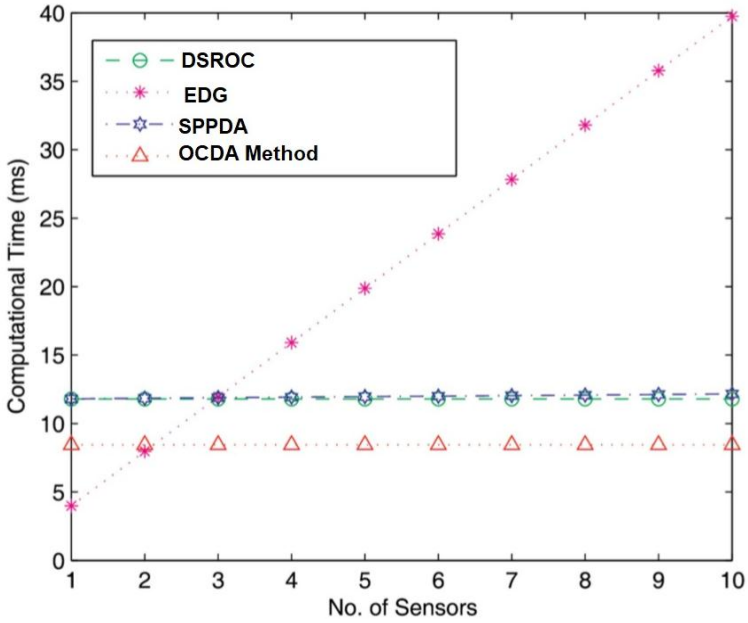

Fig 7: Comparison of Computational complexity at the Server with OCDA and Existing schemes

6. CONCLUSION

From the analysis carried out the following conclusions can be drawn

1. An optimal clustering-based Data Aggregation model for health monitoring system is proposed to improve aggregation efficiency and preserve data privacy.
2. The Security analysis demonstrates that the proposed scheme can preserve data confidentiality, data authenticity, and data privacy, while it also resists passive eavesdropping and replay attacks from malicious adversaries.
3. In the Data aggregation phase, all cluster members send its sensed data during its allotted time slot where CH eliminates the duplicates and forwards the packet to BS with secure transmission.
4. The proposed OCDA technique is suitable for health monitoring application by means of delay and energy aware data transmission.
5. The experimental results of OCDA techniques in comparison with existing techniques show the better efficiency of proposed technique with regard to computational complexity which is reduced to 8 for proposed OCDA systems in comparison to the other existing approaches which indicate high complexity (above 12-30).
6. The network life time for OCDA system is increased to 95 while the existing SPPDA is having network lifetime of 91%.

REFERENCES

[1] Gajender, A., and M. Nagaraju. 2016, "Privacy-Preserving Data Transmission Protocol for Wireless Medical Sensor Data." IJITR 4(6), pp. 4518-4522.

[2] Padmavathi, Dr G., and Mrs Shanmugapriya. 2009, "A survey of attacks, security mechanisms and challenges in wireless sensor networks." International Journal of Computer Science and Information Security, 4(1), pp. 1-9.

[3] Zhang, Changlun, Chao Li, and Yi Zhao. 2015, "A balance privacy-preserving data aggregation model in wireless sensor networks." International Journal of Distributed Sensor Networks, 11(6) pp. 937280.

[4] [4] A. Norouzi and A. Halim Zaim, 2012, "An Integrative Comparison of Energy Efficient Routing Protocols in Wireless Sensor Network", Wireless Sensor Network, 4(3), pp. 65-75.

[5] A. Shahraki, M. K. Rafsanjani, and A. B. Saeid, 2011, "A new approach for energy and delay trade-off intraclustering routing in WSNs," Computers & Mathematics with Applications, 62(4), pp. 1670–1676.

[6] N. Nguyen, B. Liu, V. Pham and Y. Luo, 2016, "On maximizing the lifetime for data aggregation in wireless sensor networks using virtual data aggregation trees", Computer Networks, 105, pp. 99-110.

[7] D. Mantri, N. Prasad and R. Prasad, 2013, "Two Tier Cluster Based Data Aggregation (TTCDA) for Efficient Bandwidth Utilization in Wireless Sensor Network", Wireless Pers Commun, 75(4), pp. 2589-2606.

[8] A. Muthu Krishnan and P. Ganesh Kumar, 2015, "An Effective Clustering Approach with Data Aggregation Using Multiple Mobile Sinks for Heterogeneous WSN", Wireless Pers Commun.

[9] Hassanalieragh, Moeen, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, and Silvana Andreescu. 2015, "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges." In 2015 IEEE International Conference on Services Computing, pp. 285-292.

[10] B. Liu and J. Jhang, 2014, "Efficient distributed data scheduling algorithm for data aggregation in wireless sensor networks", Computer Networks, 65, pp. 73-83.

[11] K. Parmar and D. Jinwala, 2016, "Concealed data aggregation in wireless sensor networks: A comprehensive survey", Computer Networks, 103, pp. 207-227.

[12] [12] L. Villas, A. Boukerche, H. de Oliveira, R. de Araujo and A. Loureiro, 2014, "A spatial correlation aware algorithm to perform efficient data collection in wireless sensor networks", Ad Hoc Networks, 12, pp. 69-85.

[13] Selvakumar Sasirekha and Sankaranarayanan Swamynathan, 2017, "Cluster-chain mobile agent routing algorithm for efficient data aggregation in wireless sensor network." Journal of Communications and Networks, 19(4) pp. 392-401.

[14] Ali, Inayat, Eraj Khan, and Sonia Sabir. 2018, "Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: A review." Future Computing and Informatics Journal, 3(1), pp. 41-50.

[15] Ramnik Singh and Anil Kumar Verma, 2017, "Energy efficient cross layer based adaptive threshold routing protocol for WSN." AEU-International Journal of Electronics and Communications 72, pp.166-173.

[16] Suneet K. Gupta and Prasanta K. Jana, 2015, "Energy efficient clustering and routing algorithms for wireless sensor networks: GA based approach." Wireless Personal Communications, 83(3), pp. 2403-2423.

[17] Kaur, Harmanjeet, Neeraj Kumar, and Shalini Batra. 2018, "An efficient multi-party scheme for privacy preserving collaborative filtering for healthcare recommender system." Future Generation Computer Systems, 86, pp.297-307.