MCEEP-BDA: Multilevel Clustering Based - Energy Efficient Privacy-Preserving Big Data Aggregation in Large-Scale Wsn

Dhanapal.R, SelvaPandian.D, Karthik.S

Abstract—In current scenario, the Big Data processing that includes data storage, aggregation, transmission and evaluation has attained more attraction from researchers, since there is an enormous data produced by the sensing nodes of large-scale Wireless Sensor Networks (WSNs). Concerning the energy efficiency and the privacy conservation needs of WSNs in big data aggregation and processing, this paper develops a novel model called Multilevel Clustering based- Energy Efficient Privacy-preserving Big Data Aggregation (MCEEP-BDA). Initially, based on the pre-defined structure of gradient topology, the sensor nodes are framed into clusters. Further, the sensed information collected from each sensor node is altered with respect to the privacy preserving model obtained from their corresponding sinks. The Energy model has been defined for determining the efficient energy consumption in the overall process of big data aggregation in WSN. Moreover, Cluster_head Rotation process has been incorporated for effectively reducing the communication overhead and computational cost. Additionally, algorithm has been framed for Least BDA Tree for aggregating the big sensor data through the selected cluster heads effectively. The simulation results show that the developed MCEEP-BDA model is more scalable and energy efficient. And, it shows that the Big Data Aggregation (BDA) has been performed here with reduced resource utilization and secure manner by the privacy preserving model, further satisfying the security concerns of the developing application-oriented needs.

Index Terms— Wireless Sensor Network (WSN), Big Data Aggregation (BDA), Energy Efficiency, Privacy Preserving, Cluster_head Rotation and Least BDA Tree.

I. INTRODUCTION

Large-Scale WSNs (LS-WSN) have been extensively distributed for several applications like health monitoring, environmental sensing, fire or smoke detection, security operations etc. Moreover, in LS-WSN, the number of deployed nodes is huge in number; hence the amount of collected data will also be greater [1]. But, the nodes are generally energy-constrained with limited storage and battery power. It is critical to develop models for processing the huge data called Big Data. The big data processing includes data collection/aggregation, storage, forwarding and analysis has been concentrated more by the scholars in present days [2].

In general, the WSN comprises cheap and effective sensor nodes that operate for environment monitoring, data accumulation, which are extensively in various applications that create great impact of daily activities of humans and machines [3]. Since the WSN plays a huge part in military surveillance, security related services and health care applications, the data that are observed by the sensors are to be more secure and private. While concerning about the data privacy, since the network is a wireless standard, supports processing with big data, is vulnerable to several privacy attacks such as eavesdropping and data leakage [4]. Specifically for LS-WSN, the secure sensed data transmission and privacy preserving have to be assured efficiently [5].

Further, due to the multi-hop communication process of sensor nodes in WSN makes the need of additional range of data transmission, may cause ‘hot spot’ problem. Hence, the utilization of energy and the residual resource of the nodes are also to be concentrated on developing a model for big data aggregation in WSN. Typically, the data aggregation function is implemented for minimizing the data size, redundancy and time of transmission [6]. Since, the sensor data are more significant, its privacy has to be preserved through an efficient model from various attacks and threats [7].

Focusing on both the efficient energy utilization and the privacy conserving of sensed data, this paper develops a model called Multilevel Clustering based Energy-Efficient Privacy-preserving Big Data Aggregation for LS-WSN. Here, the clustering model has been incorporated for efficient data transmission. That is, the nodes in the networks are framed into clusters and each cluster comprises Cluster Members (CM) and Cluster Heads (CH), to collect the sensed data and forward to the sink or Base Station (BS). The Figure 1 depicts the clustering based network design of this data aggregation model.

The proposed model works on the five phases: Cluster Formation, Energy Efficiency Model Derivation, Cluster_head Rotation, Least BDA Tree and MCEEP-BDA Algorithm. By efficient CH selection, the energy usage of the overall network can be well managed. Moreover, the sensor data is adapted with the privacy preserving model and forwarded to the cluster heads. The CHs are further responsible for efficient data aggregation and privacy preserving. In all clusters, the CH covers the obtained data by a private arbitrary number and initiates the rotation process among the CHs. This makes the sensed data more confidential and private.

Revised Manuscript Received on October 15, 2019

Dhanapal.R, Assistant Professor, Department of Computer Science Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu,India.
(Email: dhanapalramasamy.p@gmail.com)
SelvaPandian.D, Assistant Professor, Department of Computer Science Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu,India.
(Email: selvapandian79@gmail.com)
Karthik.S, Professor & Dean, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India.
(Email: profskarthik@gmail.com)

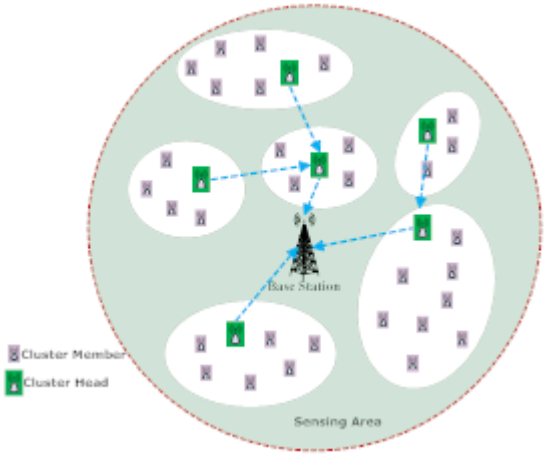

Figure 1: Clustering Model for Data Aggregation in WSN

1.1. Contributions of this Work:

- The clustering model is utilized to determine the topology of the network based on the derived energy utilization of sensors.
- The cluster heads and members supports the privacy conserving data collection and further, cluster based data aggregation model determines secure and scalable big data aggregation in LS-WSN.
- In the phase of Cluster_head rotation phase, the sensed data of each CM is concealed into the combined data, which is consistently forwarded to the next CM, till it reaches the CH. Then, the CH determines the aggregation results of the particular cluster by deducting its random number. Constantly, the aggregation function is carried out with different clusters.
- Further, Least BDA Tree is performed and the mode effectively involves in reducing the rate of energy consumption, communicational cost, avoiding the data loss and redundancy, and providing privacy over shared data.

1.2. Paper Organization:

The rest of this paper is framed as follows: Section 2 deliberates about the various related works on BDA in WSN. Section 3 gives a detailed description about the network model and the work process of the proposed MCEEP- BDA. The experimental analysis with results and comparative analysis are given in the Section 4. Finally, the paper is concluded in Section 5 with some paths for future enhancement.

II. RELATED WORKS

In [8], it has been given that the privacy preserving schemes in WSN can be categorized into four as, Encryption based, perturbation, anonymization and generalization technique. The typical end-to-end encryption model cannot be induced directly to the security model of WSN, since the sensor nodes between the source and the target could not involve in the data aggregation process. Homogeneous encryption model is given in [9], permits encrypted data aggregation without performing decryption at the middle of the delivery process. But, the data privacy could not be protected from the adjacent nodes.

In [10], Cluster based Privacy preserving Data Aggregation (CPDA) model and Slice-mix-aggregate model (SMART) model has been proposed for performing the data aggregate operation called Sum. The CPDA model agitates the acquired data using private auxiliary numbers and public seeds for determining the aggregation results. The CPDA model can be applicable for clusters that are larger in size. On the other hand, in SMART model, the data is converted into slices and forwarded to various neighbour nodes. After that, the sliced data were mixed and processed by the corresponding nodes.

K-Indistinguishable Privacy-preserving Data Aggregation (KIPDA) [11] has been designed for performing the aggregation operations such as min and max. The original data in that model has been concealed with camouflage. Further, it was stated in the paper that the potency of the privacy conservation is dependent to the message size. But, communication overhead is higher in this process. Histogram based data aggregation has been proposed in [12], which have been produced the actual data values. Corresponding to the obtained histogram, the proper results are obtained by the BS. Hence, the histogram based model in stronger in providing privacy but with reduced precision rate.

A secure mutli-level data gathering model is proposed in [13] for providing security data over the intermediate nodes, when it is decrypted. The concepts of the paper [14] presented the homomorphic encryption models. The model performed efficient data aggregation of cipher data before decryption happened. Since, the encryption function has been performed in end-to-end pattern, it provided higher data confidentiality, but, it is not feasible for the performances of MAX and MIN aggregation operations. A secret perturbation based security model for WSN was developed in [15] for secure the sensor data without interrupting the results of additive data aggregation. A tree sampling model has been given in [16] that utilized the sampling process directly to solve the aggregation concerns for functions such as add and mean that can produce appropriate response without considering the influences of the attackers.

Secure Data Aggregation Model has been provided in [17] that involved in protecting both the privacy and integrity of the aggregated sensor data. The work mainly focussed on the MIN and MAX functions of the aggregation model, without considering others. Concealed Data Aggregation model has been proposed for privacy preserving using homomorphic encryption in [18]. The model performed with additive and multiplicative homomorphic operations for determining the addition and product of the sensor information from multiple sensing nodes. But, the execution of encryption operation has become more complicated in this process, because of multiplicative homomorphic operations.

The problem of network congestion has been solved using the data aggregation process in [19]. The model was named as DyDAP (Dynamic Data Aggregation for Privacy Aware WSN). In that process, the network bandwidth corresponding to a node is lower than the data produced, the sensed data of the corresponding node has been stored in the buffer and loaded back, once the communication link become idle. Further, the work has been accomplished with the homomorphic encryption models given in [20]. Moreover, the models presented in [21], [22] and [23], discussed about the techniques for secure and reliable data sharing in communication networks. Additional functions have been added for providing data integrity, but, it makes the communication cost of the model greater.

III. WORKING PROCESS OF THE PROPOSED MCEEP-BDA MODEL

This section elaborates the work process of the proposed Multilevel Clustering based- Energy Efficient Privacy-preserving Big Data Aggregation (MCEEP-BDA). The work comprises five phases:

1. Cluster Formation
2. Energy Efficiency Model Derivation
3. Cluster_head Rotation
4. Least BDA Tree
5. MCEEP-BDA Algorithm

In the cluster formation phase, the network is separated into unshared clusters with a cluster head (CH) and number of cluster members (CM). The Energy model is derived in the second phase for proving energy efficient over the BDA process. In third phase of work, the real data of nodes are concealed with a private auxiliary number and Cluster_head rotation is incorporated for privacy preserving. In the last phase of work, the results are aggregated and transmitted to the corresponding sinks.

a) Cluster Formation:

For effective aggregation strategy, the designed network is framed into disjoint clusters. Moreover, the clusters must have the following features,

1. There must be a CH and multiple CMs in a CL and the CH must act as a data aggregator.
2. Each sensor_node must belong to different CL.
3. Cluster communication can be made through the CHs.
4. The CMs can communicate with the CHs directly.
5. The Cluster_size must be ≤3 for Cluster_head rotation

For acquiring those features, the cluster formation comprises two processes called cluster Start_up and cluster merging.

i. Energy Efficiency Model Derivation:

The total energy utilization rate of CHi is computed as in the equation (1).

$$EU(CH_i) = EU_R + EU_A + EU_T \quad (1)$$

From the equation, EUR denotes the amount of energy utilization of data packets reception forwarded from its cluster members and the other cluster heads, EUA is the consumed energy rate for received data aggregation and EUT denotes the energy consumed for transmitting the aggregated sensed data. Further, EUR , EUA and EUT are derived on the basis of the length of the data packet and the cluster_size. The equation is derived as in (2).

$$\begin{cases} EU_R = (|CL| - 1).L_{sdp}.EU_{rx} + AG_{rd}^{i+1}.L_{dp}.EU_{rx} \\ EU_A = (|CL| - 1).L_{sdp}.EU_{da} + AG_{rd}^{i+1}.L_{dp}.EU_{da} \\ EU_T = L_{sdp}.(EU_{tx} + CR^{\delta}.EU_{mg}) \end{cases} \quad (2)$$

Where, EUrx,EUda,EUtx, and EUmg denotes the energy utilization of receiving, aggregating, forwarding and magnifying the sensed data, Lsdp is the sensed data packet length in bytes and AGi+1rd denotes the average data obtained from the cluster heads. And, δ is the transmission power loss factor, which must be ≥2.

Moreover, the Energy Level of Sensor Node (SN) is defined as the amount of energy that is utilized or used by the nodes in the network. The equation for calculating the Energy Level of Sensor Node is given as,

$$\text{Energy Level of Sensor Node } EL_{SN} = \left(\frac{RE_{SN}}{IE_{SN}}\right)^{1/N_{Act}} \quad (3)$$

From the above equation, RESN denotes the residual energy of SN, IESN represents the initial energy of SN and NAct points the number of active nodes presented in the network. The probability of SNi to be the (CH) is computed as,

$$P(SN_i) = -EL_{SN} \quad (4)$$

ii . Cluster Initialization:

Based on the network based energy parameters such as the distance among the SNs, node residual energy and the energy utilization rate of each SN are considered in framing the multilevel clusters and the CHs. This ensures the communication reliability in the defined WSN and effective cluster_head rotation for privacy preserving big data accumulation. Table 1 presents the algorithm for cluster formation.

Table 1: Algorithm 1 for Cluster Formation

- Input: No. Of Iterations Max_iter;
- Output: candidate_CH_list;

1. Begin
2. Calculate Energy level of Sensor Node ELSN and forward to the sink node;
3. Sink node computes P(SNi)
4. Broadcast P(SNi) to other SNs
5. Declare Max=0;
6. While (present_iterations p_iter<Max_iter)
7. Compute the potential of node SNi based on the residual energy level
8. If potential (SNi) = potential (CH)
9. Node SNi is the cluster head
10. Else if (potential (SNi)≠ potential (CH))
11. Node SNj is the cluster head of SNi
12. End
13. Present_iterations p_iter=p_iter+1;
14. End

iii. Cluster Merging:

Following the cluster formation process, some cluster_size [CL] are considered to be lesser than 3. For feasible privacy preserving operation in Cluster_head rotation, the cluster_size is assured to be greater than or equal to 3. If the cluster_size is <3, it requires cluster merging operation. It is to be focussed that the merging process is required to start from the bottom based on the hop count of each SN, for provided linking to the complete WSN. The Figure 2 demonstrates the merging operation of the proposed model.

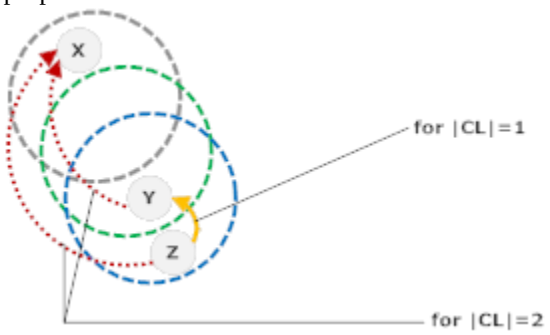

Figure 2: Merging Operation of Clusters

Based on the process of cluster formation and initialization, 3 clusters are framed (X, Y and Z) with HP as 0, 1 and 2 correspondingly. The operation of merging starts from Z to X. It the cluster_size is less than or equal to 2, then, the merging process comes into effect. If [CL] =1 , states that there is only one CH in the corresponding CL, the CH links into the CL of its respective PR. The section (2) of Figure 2 shows that the cluster Z joins with its PR, 'Y' as a CM and the 'Dt' between Y and Z does not exceed the RCL, denotes that there are two sensor nodes, a CH and a CM, both are linked with their respective CH's PR. The section (3) of Figure 2 states the clusters Y and Z joins the cluster Y's PR called 'X' and the radius of cluster X, enlarge from RCL(X) to CR. But, it is to be ensured that the distance between the X and Y does not exceed RCL, and as a result, the distance between the X and Z does not exceed the communication range of each sensor_node. After the operation performs, it is ensured that the . It is explicit that the distance between the CH and its corresponding CMs Di,j, in which 'i' denotes the CH and 'j' points the CM, holds either 0≤ Di,j≤ RCL.After the operation performs, it is ensured that the CL<3.

b) Cluster_Head Rotation Process for Privacy Preserving:

Cluster_Head rotation process is incorporated here for conserve the confidentiality of Big data in Large scale WSNs. It is considered that N0 denotes the cluster head and the cluster member set is represented as, Ni (i=1,.., m-1). 'rdi' is the real data of the node Ni. For a query qrt, each CH, N0 produces a new private auxiliary number represented as a0(t), rd' denotes the data transmitted between the clusters the clusters and rd' is computed as given in the equation 3 and the encrypted data is transmitted with a private_key PKi,j to Nj(j=(i+1)mod m). On obtaining rd'm-1 from Nm-1, N0 is used for calculating $\sum_{i=0}^{m-1} rd_i$ as in equation (4)

$$rd_i' = \begin{cases} rd_0 + a_0(t) & i = 0 \\ rd_i + rd_{i-1}' & i = 1, \dots, m-1 \end{cases} \quad (5)$$

$$\sum_{i=0}^{m-1} rd_i = rd_{m-1}' - a_0(t) i = 0, \dots, m-1 \quad (6)$$

After the computation process, path has to be designed for <N0, N1,..., Nm-1, N0> passing through each CM at least once. It is also considered that there are 'v' number of nodes with 0≤Dt0,i≤RCL, represented as Ni(i=1,.., v) and mv-1 CMs with RCL≤Dt0,j≤CR, represented as Nj(j=v+1,..., m-1). The demonstration of the rotation process is given in the Figure 3.

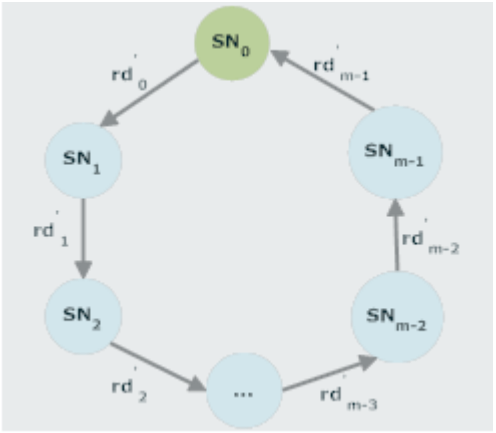

Figure 3: Cluster_Head Rotation Process

c) Least BDA Tree:

The Least BDA Tree construction comprises the formation of minimal aggregation path for multilevel clustering based communication. The algorithm is given as follows (Table 2):

Table 2: Algorithm 2 for Least BDA Tree

1. L←0 // Initialization, L is the List_of_least BDA tree
2. For each path m(i,j) ∈ candidate_CH_list
3. Sort m(i,j) into an ascending order based on Node_Weight
4. $Node_{weight(i,j)} = \frac{EY(i,j)}{RE_{SN_i}}$ (7) // $EY(i,j)$ denotes the amount of energy utilized by for forwarding a unit data to CH_j
5. End
6. For each path m(i,j) ∈ candidate_CH_list
7. If m(i,j) ∉ candidate_CH_list No_loop then
8. candidate_CH_list← candidate_CH_list ∪m(i,j)
9. End
10. End
11. Return candidate_CH_list

d) MCEEP-BDA Algorithm:

In the process of framing Least BDA Tree algorithm, the energy utilization rate of cluster head is based on the node weight as in (7). For minimizing the rate of energy utilization and communication reliability, the MCEEP-BDA algorithm has been given in Table 3. The algorithm is derived by combining the Algorithm 1 and Algorithm 2. Moreover, In Algorithm 3, the communication between the cluster heads and the cluster members with single hop and the multilevel communication is based on the additional hops of the data transmission over the network. Inter cluster communication has be effectively designed in the algorithm for efficient multilevel clustering for BDA aggregation. The algorithm is presented in Table 3.

Table 3: MCEEP-BDA Algorithm

1. Begin
2. Network Factors Initialization
3. Sink node collects the network_parameters (np) of SNs in the WSN
4. If sink node collected all (np)
5. Call cluster formation _Algorithm
6. Call Least BDA Tree_Algorithm
7. End
8. Sink node forward CH_information and information of Least BDA Tree to all SNs
9. For each SN (SNi) receives the CH_information and information of Least BDA Tree
10. If (node (SNi) is the CH)
11. Identify the next hop using Algorithm 2
12. Else
13. Determine the CH from candidate_CH_list
14. End
15. End
16. For each cluster_member
17. Performing data forwarding in each hop
18. End
19. For each cluster_head
20. Performing data forwarding in multilevel
21. Achieving Privacy Preserving using Cluster_head rotation
22. End

Following the process, the resultant aggregated data is stored in CH. Each CH forwards the Big data to its corresponding sink nodes. In this way, the BDA process is executed persistently till the aggregated data reaches the BS or sink. And, the received data is further summarized at the sink and makes the appropriate data.

IV. EVALUATION RESULTS AND DISCUSSIONS

This section describes about the performance of the proposed Multilevel Clutering based- Energy Efficient Privacy-preserving Big Data Aggregation (MCEEP-BDA) Model with respect to Energy efficiency, transmission delay, accuracy, privacy and communication overhead. Instead of real-time implementation, the protocol has been simulated for evaluation in NS-2 Network Simulation tool, respectively with 500 to 1000 sensor nodes are distributed in the sensing area of about 500x500 m2. Moreover, the results of the proposed model is compared with some traditional models called Cluster based Privacy preserving Data Aggregation (CPDA) and with the previous work of the authors such as Optimized Security Model using Enhanced Fully Homomorphic Encryption (OSM-EFHE) and Cluster-based Systematic Data Aggregation Model (CSDAM). Further, the important simulation parameters are given in the Table 4 with their corresponding values.

Table 4: Simulation Parameters and Initial Values

Parameters	Values
Simulator	NS-2
Covering Region	500 x 500 m^2
Simulation Time	900 sec
No. of SNs	Ranges from 500-1000
Transmission Range	500 m
Data Rate	0.1 Mbps
Initial Energy	10 Joules/Node
Frequency	9 Mhz
MAC Protocol	IEEE 802.11
Traffic Mode	CBR

The MCEEP-BDA model has been framed in such a way to defend against the collusion attack by multiple nodes. The chart presented in Figure 4 provides the results of the collusion of nodes based analysis. From the figure, it is shown that the privacy of the sensed big data has been protected efficiently in the proposed MCEEP-BDA than the compared models of Big data aggregation and processing. Here, the inducement of Cluster_head Rotation process aids in preserving the data privacy in a better way.

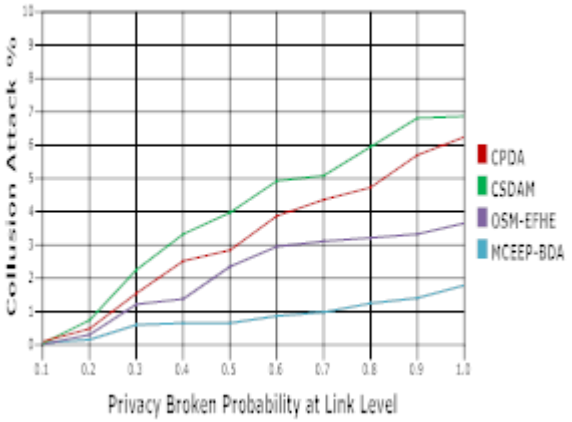

Figure 4: Collusion Attack based Analysis

Further, according to the energy efficiency model derived in section 3.2, the overall energy utilization of the proposed model is calculated with respect to their deployed sensor nodes. The computation of energy utilization has been determined in accordance with the simulation time in seconds. In average, the overall process consumed 19% of energy, at the end completing 50 seconds of simulation time. This attained result is more efficient and less than the compared model and the results of the previous works on energy consumption. The Figure 5 depicts the results of the Energy Consumption rate in Joules with respect to the simulation time.

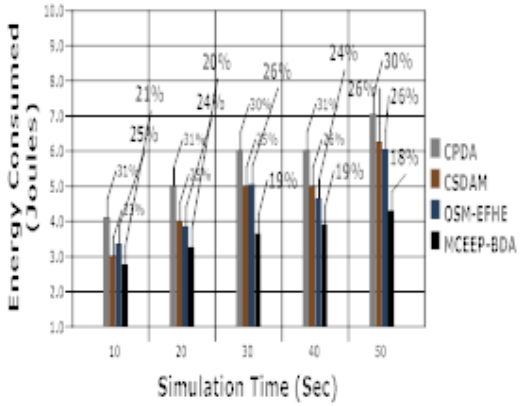

Figure 5: Energy Consumption Vs Simulation Time

Transmission delay is another important factor to be considered while performance evaluation of a model is made. It is defined as the time variation between transmitting the aggregated data and reception of the resultant data without any loss. Figure 6 provides the comparison results on transmission delay for CPDA, CSDAM, OSM-EFHE and MCEEP-BDA. It is explicit from the figure that the transmission delay of MCEEP-BDA model is lesser than others, because of its efficient cluster formation.

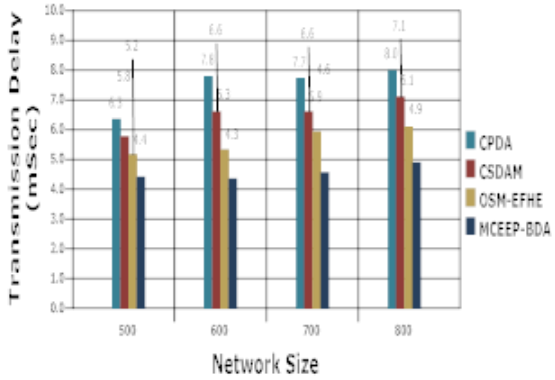

Figure 6: Transmission Delay Vs Network Size

The efficiency of the designed protocol can be evaluated on the basis of the communication delay and overhead. The minimum transmission delay and the communication overhead represents the model is more efficient. The figure 7 depicts the effect of network size in terms of communication overhead. It is observed from the chart that communication overhead increases based on the size of the WSN. Here, the communication overhead of the proposed MCEEP-BDA is lower than the other compared models for about 14%. Hence, it is efficient than the other works.

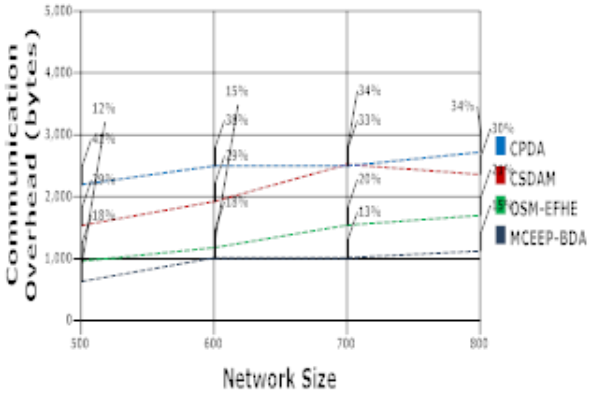

Figure 7: Comparative Analysis on Communication Overhead

The Figure 8 portrays the accuracy rate of the proposed model with respect to simulation time. Due to various attacks and collusions, the BDA models may loss some amount of data. In the proposed model, the protocol has been efficiently designed in such a way to decrease the loss of data and improves the accuracy rate. The accuracy rate of the proposed model is almost 96% in average, which is the highest value among the compared models.

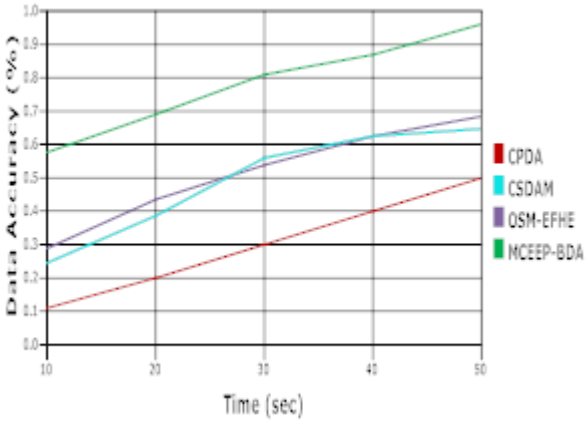

Figure 8: Evaluation on Data Accuracy

V. CONCLUSION AND FUTURE ENHANCEMENT:

In this paper, Multilevel Clustering based- Energy Efficient Privacy-preserving Big Data Aggregation (MCEEP-BDA) has been proposed for satisfying the privacy requirements of big data processing in Large-scale Wireless Sensor Networks. The main focus of the work is to secure the data privacy along with efficient energy utilization. For that, the paper incorporates an energy model, Cluster_head Rotation and Least BDA Tree model. Moreover, both the theoretical and performance evaluation of the proposed model has been made and compared with the existing models on the basis of parameters such as efficiency, accuracy, and transmission delay and data privacy. It is explicit from the result, that it outperforms the compared works in secure and efficient big data aggregation.

The enhancement can focus on providing privacy preservation for complicated queries and on implementing the process in real-time environments.

REFERENCES

1. D. Takaishi, H. Nishiyama, N. Kato, 'Toward energy efficient big data gathering in densely distributed sensor networks', IEEE Trans. Emerg. Top. Comput. Vol. 2, No. 3, 2014, pp. 388-397.
2. S. Sagiroglu, D. Sinanc, 'Big data: a review' in: Proceddings of 2013 Interna-tional Conference on Collaboration Technologies and Systems (CTS), 2013, pp. 42- 47.
3. I. Riazul, K. Daehan, K. Humaun, 'The internet of things for health care: a comprehensive survey,' IEEE Access, Vol. 3, No. 1, 2015, pp. 678-708.
4. P. Adrian, S. John, W. David, 'Security in wireless sensor networks,' Commun. ACM, Vol. 47, No. 6, 2004, pp. 53-57.
5. W. Yong, G. Attebury, B. Ramamurthy, 'A survey of security issues in wireless sensor networks,' IEEE Commun. Surv. Tutor., Vol. 8, No. 2, 2006, pp. 2-23.
6. R. Rajagopalan, P. Varshney, 'Data-aggregation techniques in sensor networks: a survey,' IEEE Commun. Surv. Tutor., Vol. 8, No. 4, 2006, pp. 48-63.
7. O. Suat, X. Yang, 'Secure data aggregation in wireless sensor networks: a comprehensive overview,' Comput. Netw., Vol. 53, No. 12, 2009, pp. 2022-2037.

8. Y. Fan and H. Chen, 'Verifiable privacy-preserving top-k query protocol in two-tiered sensor network,' Chinese Journal of Computers, vol. 35, No. 3, pp. 423-433, 2012.
9. J. Gir˜ao, D. Westhoff, and M. Schneider, 'CDA: Concealed data aggregation for reverse multicast traffxic in wireless sensor networks,' in ICC, 2005, pp. 3044-3049.
10. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. F. Abdelzaher, 'PDA: Privacy-preserving data aggregation in wireless sensor networks,' in INFOCOM, 2007, pp. 2045-2053.
11. M. M. Groat, W. He, and S. Forrest, 'KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks,' in INFOCOM, 2011, pp. 2024-2032.
12. W. Zhang, C. Wang, and T. Feng, 'GP2S: Generic privacy-preservation solutions for approximate aggregation of sensor data (concise contribution).' in PerCom, 2008, pp. 179-184.
13. Y. Yang, X. Wang, S. Zhu, G. Cao, 'SDAP: a secure hop-by-hop data aggregation protocol for sensor networks,' ACM Trans. Inf. Syst. Secur., Vol. 11, No.18, 2008, pp. 1-43.
14. C. Castelluccia, E. Mykletun, G. Tsudik, 'Efficient aggregation of encrypted data in wireless sensor networks,' in: Proceedings of MobiQuitous 05, San Diego, CA, USA, 17-21 July, pp. 109-117.
15. T. Feng, C. Wang, W. Zhang, L. Ruan, 'Confidentiality protection schemes for data aggregation in sensor networks,' in: Proc. IEEE INFOCOM, 2008.
16. H. Yu, 'Secure and highly-available aggregation queries in large-scale sensor networks via set sampling,' Distrib. Comput., Vol. 23, 2011, pp. 373-394.
17. M. Manulis, J. Schwenk, 'Security model and framework for information aggregation in sensor networks,' ACM Tran. Sens. Netw. (TOSN), Vol. 5, No. 2, 2009.
18. Girao, J.; Westhoff, D.; Schneider, M. 'CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks.' In Proceedings of the IEEE International Conference on Communications (ICC), Seoul, Korea, 16-20 May 2005; pp. 3044-3049.
19. Sicari, S., Grieco, L.A., Boggia, G., Coen-Porisini, A. 'DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks.' J. Syst. Softw., 2012, Vol. 85, pp. 152-166.
20. Castelluccia, C., Chan, A.C.F., Mykletun, E., Tsudik, G. 'Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks.' ACM Trans. Sens. Netw. 2009, Vol. 5, pp. 20-24.
21. Dhanapal, R & Visalakshi, P 2016, 'Real Time Health Care Monitoring System for Driver Community Using Adhoc Sensor Network', Journal of Medical Imaging and Health Informatics, vol. 6, no. 3, pp. 811-815.
22. Dhanapal, R & Visalakshi, P 2016, 'Optimizing Trust Based Secure Routing for Unified Efficient Resource Sharing for Large Scale MANET-TSRRS', Asian Journal of Information Technology, vol. 15, no. 19, pp. 3756-3762.
23. Dhanapal, R & Visalakshi, P 2015, 'Efficient Clustering Protocol on Ant-Bee agent for Large Scale Manet', International Journal of Applied Engineering Research, vol. 10, no. 52, pp. 349-361.