An Energy Efficient Secure Data Aggregation in Wireless Sensor Networks

Jenice Prabu A (✉ jeniceprabu.ace@yahoo.com)

Arunachala College of Engineering for Women

Hevin Rajesh D

anna university chennai

Research Article

Keywords: Wireless sensor network, Clustering, Routing, Security, Data Aggregation.

Posted Date: April 12th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-364741/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

An Energy Efficient Secure Data Aggregation in Wireless Sensor Networks

¹Jenice Prabu A, ²Hevin Rajesh D

Assistant Professor, Arunachala College of Engineering for Women, Vellichanthai

Associate Professor, St.Xaviers Catholic College of Engineering, Chunkankadai

ABSTRACT

In Wireless sensor network, the major issues are security and energy consumption. There may be several numbers of malicious nodes present in sensor networks. Several techniques have been proposed by the researchers to identify these malicious nodes. WSNs contain many sensor nodes that sense their environment and also transmit their data via multi-hop communication schemes to the base station. These sensor nodes provides power supply using battery and the energy consumption of these batteries must be low. Securing the data is to avoid attacks on these nodes and data communication. The aggregation of data helps to minimize the amount of messages transmitted within the network and thus reduces overall network energy consumption. Moreover, the base station may distinguish the encrypted and aggregated data based on the encryption keys during the decryption of the aggregated data. In this paper, two aspects of the problem is concerned, we investigate the efficiency of data aggregation: first, how to develop cluster-based routing algorithms to achieve the lowest energy consumption for aggregating data, and second, security issues in wsn. By using Network simulator2 (NS2) this scheme is simulated. In the proposed scheme, energy consumption, packet delivery ratio and throughput is analyzed. The proposed clustering, routing, and protection protocol based on the MCSDA algorithm shows significant improvement over the state-of - the-art protocol.

Keywords: *Wireless sensor network; Clustering; Routing; Security; Data Aggregation*

1. INTRODUCTION

The sensor nodes collections that communicate via wireless medium are called as Wireless sensor network. From the environment, the nodes group gathers information to achieve specific application purposes. In order to achieve maximum performance, they create connections to each other in different configurations; Using transceivers the nodes communicate each other. Ad hoc networks have few nodes without infrastructure compared to sensor networks. To track ambient conditions such as temperature, pressure, humidity, sound, vibration, location, sensor nodes are used. In many real-time applications the sensor nodes perform a variety of tasks, such as discovery of neighboring nodes, advanced monitoring, data management and processing, data collection, target monitoring, node position control and monitoring, synchronization and effective routing between base station and nodes. WSNs are consolidated into clusters. Every cluster has an aggregator called the leader sensor node. The Aggregator aggregates data in node inside the cluster and forward to the base station. It is used to boost system performance and effectively absorbs the time. The aggregation of data will helps to reduce the amount of messages sent through the network; that decreases energy consumption in the overall network. Inside the network, aggregation nodes collect data from multiple sensor nodes. Data aggregation is the mechanism through which the sensor nodes obtain the most

relevant data from already collected data and make it available to the base station with minimal energy consumption and minimum delay.

The sensor nodes run within the wireless sensor network with limited battery power. The main factor in wireless sensor networks is the reliability of the power source in large-scale wireless networks it's difficult to replace the power source with new one. The sensor nodes store the data and send it to the base station. More energy is consumed throughout the data transmission and processing; middle nodes along the route also consume more energy as the data packets are transmitted to the base station. Figure1 represents the architecture of the proposed method.

Wireless sensor network consists of sink node, which sometimes called as Base Station and many other small sensor nodes. The node observes the assigned area and aggregate the information. Aggregation helps to reduce the traffic and also minimize the energy consumption. Secure communication is the major issue in wireless sensor network. Confidentiality and integrity is the two main concerns that bother in secure data gathering. In wireless sensor networks, encryption is used to result in end to end confidentiality. To complete aggregation, the aggregator node requires decryption process to decrypt the encrypted data, which reveals the plain text at the aggregator nodes, which makes the data vulnerable to attacks.

One major factor in sensor network is to reduce the energy consumption In order to increase the lifetime of the network. In this paper, some measures have been taken to provide superior level of data gathering with high security. While data transferring or forwarding, the information of the node is constantly updated to the neighboring nodes. In between the nodes Euclidean distance is calculated to determine the neighbor node for data packet forwarding. Because of less energy consumption, the lifetime of the network is increased.

Figure 1: Architecture of the Proposed Method

In this paper , we focused on various issues in the process of data aggregation, such as delay, energy, and listed different approaches to solve these problems and then compared some techniques of data aggregation based on strategy, delay, average energy consumption and throughput. In addition, we have suggested a model based on our research that performs multi-level data aggregation and not only preserves the trade-off between energy efficiency and reliability, but also solves all database issues.

Our energy-efficient scheme has the following major advantages compared to the existing scheme:

Efficiency : Our proposed algorithm will protect data privacy with modest extra overhead, which is much lower than the existing algorithm, because our system consumes less energy.

1.2 Contribution of the research:

In this paper, we propose a Multiple cluster secure data aggregation algorithm. This algorithm chooses a set of CHs from the sensor nodes deployed in such a way that all CHs should be energy-rich nodes, distributed uniformly, and no nodes in the network are left out. Four parameters, such as node energy, node degree, intra-cluster distance and AG coverage, are taken into account by the objective function used in the proposed MCSDA algorithm. In addition, for routing the data packet from CHs to the sink, a DSDV-based routing algorithm is suggested.

The contributions in the research paper are as follows:

- i. First, evaluate the effectiveness of some of the best-known energy efficiency algorithms for WSNs.
- ii. Depend upon the comparative analysis this is figured out that Multiple Cluster Secure Data Aggregation (MCSDA) algorithm is used for the safe aggregation of data between sensor nodes in WSN. The proposed and implemented MCSDA integrate additively Cryptography encryption with multi-data processing where data belonging to different clusters are encrypted using MAC and then cipher texts are aggregated by aggregator to improve further results.
- iii. Detailed research was carried out to determine the proposed technique's effectiveness.

The paper is structured in the following terms: Section 2 defines the related work. Section 3 explains the proposed topology. Section 4 describes the proposed technique. Security is described in Section 5. Section 6 explains the performance analysis and the results, Conclusion is described in Section 7.

2. RELATED WORK

Lingaraj and Prakash [1] proposed a PARP (i.e. Power Aware Routing Protocol) which reduces energy use in congested wireless nodes. The routing protocol proposed creates a multicast tree to send a message to the destination with less effort and energy. To control multicast delivery system the proposed system selects the nearest wsn node for the perfect position to the forwarding node for preserving the energy between two neighboring goals that is placed in multicast tree. Jinhuan et al. [2] designed a novel ring and fuzzy rule-based data aggregation scheme to increase efficiency of energy while ensuring reliability in demand transfer. The network is divided into rings and processed from the outside and inside by the data aggregation ring. The proposed scheme adaptively unicasts variable number of aggregated packets copies continuously in a window according to the request transmission reliability and the imbalance of nodes energy cost. Qiyue et al. [3] designed a Unmanned Aerial Vehicle (UAV) protocol in order to increase the system-wide power effectiveness of WSNs. Unmanned Ariel vehicle is used in this approach as data mule for collecting sensor data. The protocol consists of three phases. First the network topology is constructed. Then, the sink calculated the route for data mule and selected the CHs of each cluster by executing GA. After that, the system entered the steady phase, and the data mule traversed designated path and gathered data from each cluster. Shiva et al. [4] suggested a Hybrid Algorithm which has the ability to protect data integrity and privacy through the minimization of system resources. For encryption and decryption the hybrid algorithm is used. Two methods are used in hybrid algorithms, ECC and AES. For key generation and sharing, ECC algorithm is used. The AES algorithm is used for the data encryption and decryption. Anish et al. [5] designed an OSDAP for preserving energy in WSN. Using privacy homomorphism technique the data is encrypted only at the leaf nodes. Data sensed by the leaf nodes is partitioned into pieces and then transferred to parent nodes. The intermediate nodes get the encrypted data from their corresponding child nodes and without decrypting this data, aggregates it with its own sensed data. The sink node's responsibility to process the received aggregated data, generate the required result for the targeted application and verify the integrity of data. Nirmal et al. [6] designed a Fujisaki Okamoto algorithm that makes Sybil attack firmly authenticated. A network with node group and base station is created. Every node has a physical ID in the network. The routing protocol is Ad-hoc On Demand Distance Vector Protocol (AODV). The base station send 'hello' packets to all other nodes for topology verification. At the base station the registered nodes are chosen as trusted nodes. Khalid et al. [7] designed a balanced power-aware clustering and routing protocol

(BPA-CRP) where the network topology divides the sensor area into different layers and clusters. Without overload, the clustering algorithm allows multiple rounds (a batch) of clusters. A network model is introduced to partition the sensor field into equal-sized layers and clusters taking into account the involvement of the crossover distance. Tao et al. [8] proposed Energy Optimized Secure Routing (EOSR), in which multi-factor strategy is taken for confident level of nodes, residual energy and path length. The multi-factor strategy ensures the dissemination of data through reliable nodes, as well as energy consumption. Pengwei et al. [9] designed an ASSDA (Adaptive Slice-Based Secure Data Aggregation), which could improve data slicing performance, reduce energy consumption, extend network life and maintain good privacy protection. To deal with redundant data, the essential mechanism is Secure Data aggregation (SDA). In SDA process, first a tree rooted base station is formed. Based on different roles the nodes play in the network, they divide into leaf node and aggregator node. SDA can bring down the network traffic and improve the lifetime of the nodes in WSN. Thiru et al. [10] proposed (OREA) Optimized Radio Energy Algorithm and PADSR (Power-Aware Distance Source Routing) PADSR for improving the lifetime of network. Quality of Service based routing protocols balance the energy consumption and data quality. Power-Aware Distance Source Routing (PADSR) determines the performance evaluation of Quality of Service. A New adaptive aggregation and compression scheme was developed by Ikjune et al. [11] for solar powered WSNs. In which, data in the node is aggregated, then data is sensed and compressed then transmits only when it receives more energy than it can store. If no solar energy is available, especially at night, then the node end transmitting but continues sensing. This approach reduces the number of nodes that black out and thus allows more data to be obtained. For cluster based sensor network, Muthukumaran et al. [12] designed an ENEFC (energy-efficient clustering). The proposed method is suited for periodical data collecting functions. This approach determines that, using suitable cluster head selection process how clusters are formed. Cluster sharing will reduce energy consumption and prolong network life. Haythem et al. [13] designed data aggregation in a secured scheme depends upon homomorphic primitives, Should protect the integrity and confidentiality of end to end data. By using (HMACs) Homomorphic Message Authentication Codes, this approach can detect false data right away in conjunction with the Elliptic Curve Elgamal algorithm by verifying data integrity. Mohamed et al. [14] proposed an itinerary planning algorithm, for Mobile Agents (MA) depend upon Cluster heads (CH). This method defines that planning itinerary in between Cluster Heads (CH), rather than planning itinerary in between the sensor nodes (SN). First of all, group SNs in clusters depend upon the density of SNs then select some SNs as CHs. Then, itineraries for MAs in between CHs depends upon Minimum Spanning Tree(MST). At last, dispatch an optimal number of MAs for data collection and gathering from CHs. Prathima et al. [15] designed a (SDACQ) Secured Data Aggregation for Coexisting Queries, which allows parallel coexisting queries from the source to be disseminated in an authenticated manner and aggregate the data belonging to coexisting queries into a single packet in wireless sensor networks. Using additively homomorphic encryption, Cluster heads collect data from sensor nodes that is encrypted.

Some of the limitations in the existing work were identified after an exhaustive literature review of various research papers. The existing approaches do not provide efficient to avoid high energy consumption and security. This causes the aggregator to use considerably more energy relative to other sensor nodes and this can die earlier. Aggregators cannot communicate with them directly because these are far from the base station.

The paper is structured in the following terms: Section 3 defines the proposed topology. Section 4 explains the proposed technique. Security is described in Section 5. Section 5 6explains the performance analysis and the results, Conclusion is described in Section 7.

3. PROPOSED TOPOLOGY

In WSN, 'N' sensor is randomly deployed. In which, the nodes and base station are static. All nodes are static in nature including base station.

In network, the resource rich device is Base station, with a long transmission power which enables its message to be sent to any sensor node. A unique identification number has been given to each node. The Network nodes track the environment and data will be communicated with the base station. It is considered that the location coordinate and its value are constant in all sensor nodes. In this paper multiple clusters Secure Data Aggregation (MCSDA) is proposed, in which cluster based WSN is designed. Each Aggregator (AG) in the cluster aggregates the cluster member sensed data (CMs) and then transmits the sensed data to the base station. Each nodes energy consumption depend upon the data packet size, and source node distance. To forward t-bits of the data packets to the remote receiver node from the sensor node, The following equations calculate a sensor node's total energy consumption

$$E_T(t, d) = \begin{cases} t \times E_e + t \times \epsilon_{as} \times d^2, & \text{if } d < d_0 \\ t \times E_e + t \times \epsilon_{mm} \times d^4, & \text{if } d \geq d_0 \end{cases} \quad (1)$$

Once the receiver node receives t-bits of data packet on a sensor node, it receives energy. The following equation calculates the receiver nodes energy consumption

$$E_R = t \times E_e \quad (2)$$

Where, E_e value represents dissipated energy per bit while the receiver or transmitter circuit is being executed, ϵ_{as} represents free-space amplification coefficient of the transmission amplifier and ϵ_{mm} is the multipath model. The threshold transmission is represented as d_0 and its value is $\sqrt{\epsilon_{as} / \epsilon_{mm}}$.

Figure 2: Flow diagram for different phases of the protocol proposed

4. PROPOSED METHODS FOR CLUSTERING AND ROUTING

The proposed method describes Multiple Cluster Secure Data Aggregation Algorithm (MCSDA), followed by Destination Sequence Distance Vector Protocol (DSDV) based routing algorithm to bring data aggregated from AGs to Base Station. The Destination Sequenced Distance Vector (DSDV) is a hop-by - hop vector routing protocol that needs routing updates to be transmitted frequently by each node. This is a table guided algorithm based on modifications made to the routing function of Bellman-Ford. A routing table with entries for each of the destinations in the network and the number of hops required to reach each of them is maintained by each node in the network. Fig 2 shows the flow diagram of the different phases.

4.1 Clustering and routing

To transfer the data packets over the network DSDV protocol is used. The DSDV sends the packets to the nodes using routing table. The routing table contains the details of Destination, node ID, node location, next hop node and hops number. Every entry in the routing table is marked in sequence which is generated by the destination node. After completion of this process, the base station generates a network topology and the clustering process is done by Multiple Cluster Secure Data Aggregation Algorithm.

4.2 MCSDA

Clustering process is done at the base station after routing phase. In this phase, MCSDA-based clustering is used to determine the optimal state of AGs. Cluster formation in the network is initiated after determining the optimum location of the AGs. After that Fitness function is concerned for selecting the best solution and the process of cluster formation.

4.2.1 Fitness function for clustering definition

A test set for optimal position AGs should be selected to maximize network life. To achieve the objective, a fitness function is generated; four parameters are involved, such as residual energy, node degree, cluster distance and coverage ratio. The definition and derivation of these parameters are shown below

a) Node energy (N_{ene})

To select the Aggregator (AG), the node is selected as the best candidate with maximum energy by using proposed clustering algorithm. Rather than CM, the AG should have additional responsibility such as managing the cluster and data aggregation. In accordance with balanced Network energy consumption, it has better energy budget. Sensor nodes residual energy is defined as,

$$\text{Min } N_{ene} = \sum_{k=1}^n \frac{1}{E_{AG}} \quad (3)$$

Here,

E_{AG} is the kth AG's residual energy, the number of AGs is n.

b) Node Degree (N_{dg})

The number of sensor nodes is defined by the node degree which can be reached from AG. Node Degree is also used to balance the load on the AG.

$$\text{Min } N_{dg} = \sum_{k=1}^n |CM_k| \quad (4)$$

Here, $|CM_k|$ is the number of cluster members of kth AG.

c) Inter-cluster distance (D_{int})

The distance of an AG from its CMs is specified as average inter-cluster distance. D_{int} also ensures the clusters quality and increases the quality of connectivity between AG and CMs.

$$\text{Min } D_{int} = \sum_{i=1}^n \left[\frac{\sum_{k=1}^{|CM_i|} d(AG_i, CM_k)}{|CM_i|} \right] \quad (5)$$

Here, $d(AG_i, CM_k)$ is the Euclidean distance between ith AG and kth CM.

d) Coverage of the AG (CAG)

AGs aim is to eliminate sensor nodes which are not clustered and ensure whether some left-out sensor nodes participate in the clustering. The parameter decreases the number of left out nodes and that cannot be part of any cluster. Consequently, the selected AGs coverage is enhanced. This parameter is defined as,

$$\text{Min } AG_{cov} = \frac{(N-n) - \sum_{i=1}^n |CM_i|}{\sum_{i=1}^n |CM_i|} \quad (6)$$

Whereas, the total number of sensor node is represented by N, n indicate the number of AGs and $|M_i|$ denotes the number of cluster members in the ith cluster.

Fitness function (F) is defined as the weighted sum of the above four parameters. The Fitness function (F) is represented as

$$F = w_1 \times N_{ene} + w_2 \times N_{dg} + w_3 \times D_{int} + w_4 \times AG_{cov} \quad (7)$$

Linear programming formulation for AG selection

$$\text{Min } F = w_1 \times N_{ene} + w_2 \times N_{dg} + w_3 \times D_{int} + w_4 \times AG_{cov} \quad (8)$$

Subject to

$$N_{ene} > E_{tn} \quad (9)$$

$$N_{dg} \leq NE_{tn} \quad (10)$$

$$D_{int} < T_{mtr} \quad (11)$$

$$w_1 + w_2 + w_3 + w_4 = 1, w_1, w_2, w_3, w_4 \in (0,1) \quad (12)$$

Where, E_{tn} represents the threshold node energy NE_{tn} represents the threshold value of node degree and T_{mtr} represents the sensor nodes maximum transmission range.

4.2.2 Cost function

Depend upon the cost function each host cost is evaluated and it is shown as,

$$y1 = \max_{j=1,2,3,\dots,j} \{ \sum d(m_k, AG_j) / |j| \} \quad (13)$$

$$y2 = \sum_{k=1}^N E(m_k) / \sum_{j=1}^j E(AG_j) \quad (14)$$

$$\text{Cost} = \beta * y1 + (1 + \beta) * y2 \quad (15)$$

The function y1 represents the maximum average distance of Euclidean nodes to their AG. C_j Represents the number of nodes associated within common cluster range. The total energy ratio of all AG to total energy of all the nodes on the network is represented by the function y2. The β value is 0.5. The y1 and y2 functions minimum value helps to reduce the intra-cluster distance and to choose optimum AG that lowers energy consumption.

4.2.3 Working of MCSDA based AG selection Algorithm

MCSDA algorithm, explains the process of Aggregator (AG) selection. By using this method, we allocate that N sensor nodes are there in the network, in which we select m sensor nodes as AGs. The MCSDA algorithm has following steps

Step1: Initialization

Using equation (7), each sensor nodes fitness value is calculated. Based on MCSDA algorithm, the sensor nodes are chosen from S as the candidates most suitable for AGs. The nodes which were selected are the suitable candidate to become AGs. Let the selected node is denoted as E_AG. After that let assume the total number of host and sensor nodes n are chosen as AGs. From the E_AG list each host is populated with n sensor nodes. All desirable sensor nodes have unique ID in the network. Then the cost of each host is calculated in equation (15). The cost functions highest value is chosen as the best host. The best host chosen is denoted as H_b . The host with best set of AGs is denoted by H_b . After completion of this phase, iterative process of MCSDA algorithm will be defined.

Step 2: MCSDA Iterative process

In MCSDA iterative process a new population is created. To generate new population, the H host set is created, each packed with n sensor nodes, choose from E_AG. After that we have to evaluate the cost function in eqn (14) and then it selects a new host with the highest cost function value. The selected host is denoted as H_n . If H_n is higher than H_b then replace the value of H_b by H_n . Step2 repeats until Max_Gen is reached.

Step 3: Best Solution

After MCSDA iteration process is complete, data gathering round can get best host as a set of best-positioned AGs, providing the best-positioned AGs.

4.2.4 Cluster formation

After best position AGs are selected, the cluster formation process is started. In this process, using neighboring AGs non-cluster nodes form a cluster together. In the network, the energy consumption plays a vital role in cluster generation process.

Cluster node of joining the AG, includes parameters such as AG residual capacity, AG node degree and AG node distance from the base station node. The cluster joining (AG_Join_Cost (k,i)) cost function is represented as follows

$$AG_Join_Cost(k,i)=\alpha_1 \times E_{AG_i} + \alpha_2 \times \frac{1}{NE_{AG_i}} + \alpha_3 \times \frac{1}{d(AG_i,bs)} \quad (16)$$

Where, $\alpha_1 + \alpha_2 + \alpha_3 = 1$ and $\alpha_1 > \alpha_2 + \alpha_3$. E_{AG_i} denotes the residual energy and NE_{AG_i} denotes the node degree of kth AG. $D(AG_k, bs)$ is the distance from the base station to the ith AG.

To balance energy consumption near the base station, a minimum number of clusters are formed and a maximum number of clusters are generated from the base station to the AG, which means that the cluster near the base station has a smaller degree of AG compared to the distant cluster. The cost function is calculated for each non-cluster node of joining the AG, including parameters such as AG residual energy, degree of AG node, and AG distance from the base station node. The cluster joining (AG_Join_Cost (k,i)) cost function is represented as follows

$$AG_Join_Cost(k,i)=\alpha_1 \times E_{AG_i} + \alpha_2 \times \frac{1}{NE_{AG_i}} + \alpha_3 \times \frac{1}{d(AG_i,bs)} \quad (17)$$

Where, $\alpha_1 + \alpha_2 + \alpha_3 = 1$ and $\alpha_1 > \alpha_2 + \alpha_3$. E_{AG_i} denotes the residual energy and NE_{AG_i} denotes the node degree of kth AG. $d(AG_k, bs)$ is the distance between ith AG and the base station.

Algorithm: MCSDA based Aggregator selection Algorithm

Input:

- i. $S=\{s_1, s_2, \dots, s_N\}$ S is the collection of sensor nodes and N is the Total number of sensor nodes

Output:

Optimal solution of AGs

Step1: Initialization

- i. for k=1 to N
Using eqn.7 calculate the fitness of each node

4.3 Routing Algorithm using Destination Sequence Distance Vector protocol

Using multihop communication, the sensor data is collected from its cluster members (CMs) from each aggregator (AGs) and the data is then forwarded to the base station. The problem in routing can be solved by using DSDV protocol. In order to choose the best route from AGs to base station an objective function is derived, which contains next-hop nodes residual energy, distance of next-hop node from the base station and length of the path.

4.3.1 Routing algorithm Description

DSDV protocol is used in the proposed routing algorithm. In this algorithm, network nodes determine their hop count from base station. Then the chance of selecting node i as its next hop node is calculated by $P(k, i)$ by following expression from node k to base station

$$P(k, i) = \begin{cases} \frac{hp_k}{\sum_{j \in N_k} hp_k} \times \frac{E_k}{\sum_{j \in N_k} E_j} & \text{if } i \in N_k \end{cases} \quad (18)$$

Here, N_k denotes the list of neighboring nodes of node k . The hop count of node k and i is denoted by hp_k and hp_j respectively. The residual energy of node k is denoted by E_k .

After probability $P(k,i)$ selection, DSDV protocol is initialized. In which all possible routes from the source node to the BS(Base Station) is included. AG nodes are the intermediate nodes in between source node and base station. The DSDV protocol represents forwarding path which contain AGs. Length of distance vector is illustrated in equation (17)

$$DV = \left\{ \begin{matrix} X_1 \\ X_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ X_K \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ X_{DV} \end{matrix} \right\} \left\{ \begin{matrix} (S, X_{1,2} \dots \dots, d) \\ (S, X_{2,2} \dots \dots, d) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ (S, X_{k,2} \dots \dots, d) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ (S, X_{DV,2} \dots \dots, d) \end{matrix} \right\} \quad (19)$$

After Distance vector is initialized energy consumption of each path is represented by x_k . The vector x_k paths which consume more energy are H_{wp} . y^1 is created based on DSDV. The source node of y^1 is the first element in order to select the next hop, select the random number R_1 from 0 to 1. If R_1 value is less than DSDV, then randomly choose the next hop. Otherwise the next-hop is chosen from the previously selected neighbor node. This method has to be repeated until reaching the destination node.

5. SECURITY IN OUR NETWORK

The base station in our network has enough resources and it is trustworthy. The sensor nodes on the other hand are very poor in resources and it is not trustworthy. Data aggregation technique must be used for energy saving and also achieve the following security goals.

5.1 Data Privacy:

Data privacy must be secure because compromised data leads to incorrect aggregation results.

5.2 Confidentiality of data

The provision of confidentiality ensures that sensitive information is well secured and not exposed to unauthorized third parties. Confidentiality refers to protection of information from being accessed by unauthorized parties. In other words, only those eligible to do so will have access to sensitive information. Nodes can communicate data which is highly sensitive. The standard approach for retaining sensitive data is to encrypt the data with a code that is intended only for the recipients and thus confidentiality.

5.3 Data authentication

Data is thought to be authentic only if the guaranteed sender has sent the data else it is accepted as unauthenticated and ignored. We accomplish data authentication utilizing special identity marker and a different, secret key is created for every sensor node. For many applications in sensor networks, Message authentication is important. A secret key is shared by the sender and receiver for processing a message authentication code (MAC) for all data communicated. At the point, when the message arrives with the right MAC the receiver knows that the sender has to return it.

5.4 Integrity of data

The integrity of data is the maintenance and confirmation of the accuracy and consistency of data throughout its life cycle and an important aspect of designing, implementing and using any system that stores, processes or recovers data. Validation of data is a precondition for integrity of the data. Integrity of the data is against corruption in the data. In short, data integrity is aimed at preventing unintended changes in information. Integrity of data is the discipline that protects data from unauthorized parties.

5.5 Model of attacks

Some of the boundary adversaries are presumed to break the integrity and privacy of aggregation result.

Node compromise: A sensor node enables the attacker to access all the contents and manage communication with the neighbors as well. Compromising node may have option to change the data by their own.

Replay attacks: In replay attacks, an attacker intercepting different exchanged packets maliciously repeats the transmission in between the networks.

Cipher text analysis: Analysis of encrypted packet is the most basic passive attack. In such analysis the opponent seeks information only encrypted. Ensure the system that sensitive information (plain text, key) cannot be obtained from the encrypted data.

Unauthorized aggregation: The unauthorized nodes of the sensors will communicate with the nodes of the sensor and then the false data will be aggregated with more cipher text and sent to the network.

Security tools: To provide privacy, encryption method is used which allows calculation over encrypted data. Aggregation functions can be applied to the encrypted data, thereby reducing sensor workload. By using the Message authentication code (MAC) the base station can verify data integrity and detect false data.

5.6 Construction of MAC

The message m s are shaped as p bits segments. Let $m=2^p$, then space for message is S_m^p . The shared key KS composed of (key1, key2). The key space of key1 and key2 is $KS1$ and $KS2$ respectively. The identity of space nodes is denoted by I . The two pseudo random functions are

$$RF1: \rightarrow S_m^p \quad (20)$$

$$RF2:(KS2) \rightarrow S_m \quad (21)$$

The computation of MAC_l as follows

$$a_l = RS1(key1)$$

$$b_l = RS2(key2, id_l)$$

$$MAC_l = a_l m_{s_l} + b_l \quad (22)$$

The aggregated MAC is denoted as follows

$$AMAC = \sum_{l=1}^v W_l MAC_{s_l} \in S_m \quad (23)$$

The weight of the message m is denoted by W .

5.7 Cryptographic Encryption

The elliptic curve ElGamal(EC) is an asymmetric algorithm in cryptography. The advantage of using cryptographic encryption key is publicly known. The message is mapped with the Cryptographic Elliptic Curve (CE). Before a text is encrypted using EC, first map plaintext with CE. A simple mapping mechanism in which the plaintext t is multiplied by point P to obtain the CE point T_p is used. The addition of plaintext is equal to the addition of CE.

Algorithm 2 : Cryptographic Encryption

Require : Public key K , plaintext t

Ensure : cipher text (C, T)

1. choose random $k \in [1, p-1]$
2. $M = \text{map}(t)$
3. $C = fP$
4. $T = P + kK$
5. return (C, T)

Cryptographic Decryption

Require : Private key e , ciphertext (C, T)

Ensure : plaintext t

6. $M = eC + T$
7. $T = \text{map}(M)$
8. return t

5.8 Aggregation of Secure Data

In aggregation of secure data, WSN addresses the result of aggregation by the network's aggregator nodes or sensor nodes. Data confidentiality and data integrity are key security requirements. In aggregation of secure data in

WSN, several drawbacks are obtained in the existing algorithms which results in high computation due to inefficiency and communication overheads. This problem occurs when malicious nodes are detected. Aggregation of data, integrity of data, confidentiality of data and detection of false data is not combined in the existing algorithms. The proposed method identifies the false data as soon as possible. So the communication overhead can be decreased, low energy consumption is obtained, in this way the life of sensor nodes and networks extends. This section introduces a new secure cryptographic encryption-based data aggregation scheme to address the security issue in the wireless sensor network. Aggregation of secure data scheme introduces MAC algorithm, which protects the confidentiality and integrity of end-to-end data based on the ElGamal data encryption algorithm combined with MAC to check the integrity of the data. Secure data aggregation model consists of following process generation of Key, Encryption, MAC method, Aggregation and Verification. Three categories are distributed in the implementation of these processes.

- **Cluster member(CMs) :**

Each sensor node encrypts their data and generates MAC. And then sends information to aggregator (AG). Some of the operations executed by the sensor nodes are Key generation, MAC and encryption process.

- **Aggregator(AG) :**

The cipher texts are aggregated by the aggregator and MACs from the sensor node. Such process is done in the Aggregator (AG).

- **Base station :**

Base station confirms the results obtained from the aggregators in order to check the validity. So, the conclusive outcome is operations executed by the base station.

Equipment	Process
Cluster Member	Encryption and MAC generation
Aggregator	Aggregation process
Base station	Verification process

Figure3. MAC block diagram

5.8.1 Key Generation

The base station generates keys, which are used to encrypt data by different cluster members. Give E, set of CE points and large prime (l1, l2, l3), then generate a tuple (l1; l2; l3; E). Then randomly selects three points (r₁; r₂; r₃) from E.

Calculate points D = l2l3r₁, G = l1l3r₂, and M = l1l2r₃. Such that D, G and M order is l1, l2 and l3 correspondingly. The public and private keys, P_k and S_K is defined as follows

$$P_k = (E, M, G, D) \quad (24)$$

$$S_K = \{(l1, l3)(l2, l3)\} \quad (25)$$

To encrypt the plaint texts, the base station transmits public key P_k to the cluster members in the network.

5.8.2 Cluster member operations

By applying ElGamal algorithm, each cluster member in the cluster generates the ciphertext and generates from the plain text a valid MAC, which is sent to the aggregator with the cipher text.

Algorithm 2 : Encryption and MAC generation process

Encryption

1. choose random $k \in [1, p-1]$
2. $M = \text{map}(t)$
3. $C = f * P$
4. $T = P + k * P_k$
5. Ciphertext = (C, T)

MAC generation process

The message ms is formed as p -bit segments. Let $m=2^p$, then S_m^p is the message space. The shared KS composed of (key1, key2). KS1 and KS2 are the key space of key1 and key2 respectively. The identity of node space is denoted by I . The two pseudo random functions are $RF1:KS1 \rightarrow S_m^p$ and $RF2:(KS2 \times I) \rightarrow S_m$.

The following MAC_i is calculated as

$$a_i = RS1(key1)$$

$$b_i = RS2(key2, id_i)$$

$$MAC_i = HR_i a_i ms_i + b_i$$

Where HR is the secret header information that identifies the sensor node in a unique way

5.8.3 Aggregation process

In aggregation process, MAC is applied to protect the confidentiality and integrity of end to end data. In order to provide message authentication, cryptographic technique is Message authentication code. The small piece of information used to confirm that the message came from the sender and was not altered. MAC ensures both the validity and authenticity of a message data, allowing verifiers to detect any changes to the message content. The MAC approach primarily aims at segmenting the data packets into small segments and is used to authenticate a message. Authentication means sender will send a message or data to a receiver with authenticator (pair of key values) and the message should not be changed. In order to establish the MAC process, the sender and receiver share a key k . In key generation, Key k randomly selects key from space. The nodes use the MAC algorithm, input the message and the shared key ks and create a MAC. Signing, is the efficient process which returns a MAC generated from the key and the message. Together with the MAC the nodes forward the message. The message sent to the aggregator is clearly concerned with authentication and confidentiality of the origin of the message. The message needs encryption if the confidentiality is required. On receiving the message and MAC, the aggregator sends the message received and the key ks exchanged to the MAC algorithm and recalculates the MAC value. In Verifying process, the Aggregator efficiently verifies the authenticity of the message (i.e) check whether the message is duplicate or not. Now, the Aggregator examines the equality of newly calculated MAC from the sender node with the received MAC. If the received message matches then, the message will be accepted by the aggregator and the message will be sent by the intended node. If the MAC send by the node does not match with the computed MAC, the aggregator decides that message is a modified message or if it is the false origin. At last, the recipient believes confidently the message is not real. If the message is genuine, then the Aggregator transfers the message to the base station. MAC is same as message digest, Message digest are intended to protect the trustworthiness of a piece of data or media to detect changes and alternations to any part of a message. A shared key ks and it is used for encryption. Text authentication is about protecting the credibility of a text, validating an originator's identity, non-repudiating the origin.

5.8.4 Verification process

The base station checks the aggregated result it receives by decrypting it. The below fig shows that how message transfer securely. MAC generation of a message using shared key ks . Sensor nodes send the original message and $MAC(H1)$ to the aggregator. Aggregator receives the original message and MAC. Receiver calculates the $MAC(H2)$ using shared key ks and original message. Compare $H1$ with $H2$. If $H1$ is not the same as $H2$ the message will be changed. If $H1$ is equal to $H2$, then it will not alter the message.

Figure 4: Verification process

6. PERFORMANCE ANALYSIS

The performance evaluation is done to check how far the proposed protocol works compared with other protocols. The most commonly used simulation platform is NS-2. Network simulator is used to simulate the performance analysis of the proposed protocol. Initially, this section outlines a brief definition of performance measurements this section then describes the brief definition of the simulation environment and the various parameters used in the experiments. A detailed outcome of the proposed protocol will be analyzed and the comparison illustrated. The results are parallel with IF, PIP and LEACH protocol.

Table 1

Parameters	Value
------------	-------

Simulation area	200×200
Number of nodes	500
Node communication range	250m
Fixed code rate	1Mbps
Packet size	512byte
Node initial energy	50J
Simulation time	500s

6.1 Performance Metrics

The following measures are used with IF, LEACH, and PIP to conduct detailed performance analysis of the proposed MCSDA protocol.

- **Total Energy Consumption(E_{total}):**

It is specified as the total energy consumption in the network following k rounds of data collection from the area-of-interest. This is the percentage of the total amount of energy taken by the nodes from the source node to the base station. The minimum value is taken or considered as the better performance.

$$E_{total} = \sum_{i=1}^N E_{i,k}$$

Where $E_{i,k}$ defines total energy consumption per node i after k number of rounds of network data collection. In the network, N is defined as the total number of nodes.

- **Lifetime of Network:**

It is defined as the number of data collected by a WSN. Longer network stability time is an important requirement, since the loss of data from one sensor node affects the final results. The lifetime of network is calculated as

$$t = \frac{E_0}{P}$$

where E_0 is the initial energy of battery , P is the power consumed by the device and t is the lifetime.

- **Throughput**

It is the sum of data packets which are sent from source node to sink node over a specified period of time. The maximum value is taken or considered as the better performance.

- **Delivery of packet**

The percentage of packets in the source node obtains with the specified time against the amount of packets created by the nodes in the WSN. The maximum value is taken or considered as the better performance.

$$PDR = \frac{P_{Rec} \times 100}{\sum_{i=1}^n P_{Gen}}$$

P_{Rec} represents the total number of packet received by the sink node. P_{Gen} is the total number of packets generated by the source node and n is the number of sensor node.

- **Delay**

Time utilized by a packet to reach destination node from sink node. The time delay faced by each node is calculated against the sum of packets obtained by sink. The minimum value is taken or considered as the better performance.

$$D = \frac{\sum_{i=1} P_{Rec}(T_{Rec} - T_{Trans})}{P_{Rec}} \quad (29)$$

Where T_{Rec} defines the time when data packet received by the sink node, T_{Trans} represents the time when data packets generated by each source node.

6.2 Result Analysis

6.2.1 Analysis of performance in terms of total energy consumption

In the performance analysis, the simulation experiment is carried out in a scenario in which 50 nodes are presented uniformly on a square sensing field of dimension 200×200

Figure 5: Performance analysis in terms energy consumption

Fig 5 shows that the energy consumption will grow rapidly. In which, the energy consumption of the different aggregation algorithms is varied as the number of nodes. The suggested protocol MCSDA's energy consumption is correlated with IF[22] and LEACH[19] and PIP[29].

Figure 6: Processing Time

Fig 6 shows the processing time of proposed protocol MCSDA. In the simulation, the processing time of PIP[29],IF[22] and LEACH[19] is more when compared with MCSDA.

Figure 7: Overall cluster performance

Figure 7 shows the overall cluster performance. Where the number of packets received at the base station is greater in the proposed method. The number of packets is determined by energy consumption, the more stable the energy consumption is, the more packets received by the base station. This improvement is achieved by the Cluster head selection method, which ensures a balanced cluster head generation across all clusters. Another explanation for the change is that MCSDA is adjusted to ensure that all sensor nodes are roughly the same volume.

Figure 8: Throughput

Figure 8 shows the throughput of proposed protocol MCSDA, PIP and LEACH protocols. In a network, each routing protocol has a relatively large throughput. The paper proposes the largest throughput of the routing protocol, in which the routing protocol of the paper selects the node of confidence to carry out the data transmission while routing. Comparing with PIP[20] and LEACH[19], the proposed protocol MCSDA has higher throughput.

Figure 9: Delay

Fig 9 compares the average delay of MCSDA, PIP and LEACH protocols. In this simulation, MCSDA attains the less delay when compared with PIP and LEACH.

Figure 10: Energy Consumption

Figure 10 shows energy consumption by MCSDA against IF and LEACH protocols. MCSDA consumed low energy when comparing with IF and LEACH.

MCSDA performance is assessed on the basis of energy life, average network energy consumption individually and per packet basis, and network throughput. The performance of MCSDA is compared to the existing

routing protocols such as LEACH[19], IF[22] and PIP[29], Compared to LEACH, where MCSDA shows an impressive performance in terms of improving network life and network throughput, MCSDA shows better results.

7. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, two major problems are addressed energy consumption and security that are to be solved by using Multiple Cluster Secure Data Aggregation Algorithm. Secure data aggregation of multiple clusters is used to safely aggregate the data between sensor nodes in WSN. MCSDA additionally integrate Cryptography encryption with multi-data processing where data belonging to different clusters are encrypted using MAC and then cipher texts are aggregated by aggregator. The MCSDA algorithm also uses fitness function. The algorithm's efficiency is tested in different scenarios, and some well-known clustering-based algorithms compare the experimental results. Under different network scenarios, the results of the simulation confirm best performance of the algorithm proposed. MCSDA performance is assessed on the basis of energy life, average network energy consumption individually and per packet basis, and network throughput. The performance of MCSDA is compared to the existing routing protocols such as LEACH, IF and PIP, Compared to LEACH, where MCSDA shows an impressive performance in terms of improving network life and network throughput, MCSDA shows better results. The simulation results also show the effectiveness of the MCSDA protocol. The overall ratio of packet delivery rate is achieved to 97.69% as well as the network throughput and energy consumption is amended to 96.3%. The future of the work is scheduled to strengthen our MCSDA framework with Scalability that would expand large-scale wireless network support.

Declarations

Funding

No funding was received for this submission

Conflicts of interest/Competing interests

No conflict of interest exists

Availability of data and material

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Code availability

Code will be available to authors based on request

References

- [1] M. Lingaraj, and A. Prakash. "Power Aware Routing Protocol (PARP) to Reduce Energy Consumption in Wireless Sensor Networks."
- [2] 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* 6 (2018): 71857-71870.
- [3] Qiyue Wu, Peng Sun, and Azzedine Boukerche. "An Energy-Efficient UAV-Based Data Aggregation Protocol in Wireless Sensor Networks." In *Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 34-40. ACM, 2018.
- [4] Shiva Prakash, and Ashish Rajput. "Hybrid cryptography for secure data communication in wireless sensor networks." In *Ambient Communications and Computer Systems*, pp. 589-599. Springer, Singapore, 2018.
- [5] Anish Soni, and Dr.Rajneesh Randhawa. "OSDAP-Optimized and Secure Data Aggregation Protocol for Wireless Sensor Networks." *International Journal of Applied Engineering Research* 13, no. 5 (2018): 3027-3033.
- [6] K. Nirmal Raja, and M. Maraline Beno. "Secure data aggregation in wireless sensor network-Fujisaki Okamoto (FO) authentication scheme against sybil attack." *Journal of medical systems* 41, no. 7 (2017): 107.
- [7] Khalid A. Darabkh, Mohammad Z. El-Yabroudi, and Ali H. El-Mousa. "BPA-CRP: A balanced power-aware clustering and routing protocol for wireless sensor networks." *Ad Hoc Networks* 82 (2019): 155-171.
- [8] Taochun Wang, Xiaolin Qin, Youwei Ding, Liang Liu, and Yonglong Luo. "Privacy-preserving and energy-efficient continuous data aggregation algorithm in wireless sensor networks." *Wireless Personal Communications* 98, no. 1 (2018): 665-684.
- [9] Pengwei Hua, Xiaowu Liu, Jiguo Yu, Na Dang, and Xiaowei Zhang. "Energy-efficient adaptive slice-based secure data aggregation scheme in WSN." *Procedia Computer Science* 129 (2018): 188-193.
- [10] J. T. Thirukrishna, S. Karthik, and V. P. Arunachalam. "Revamp energy efficiency in homogeneous wireless sensor networks using optimized radio energy Algorithm (OREA) and power-aware distance source routing protocol." *Future Generation Computer Systems* 81 (2018): 331-339.
- [11] Ikjune Yoon, Hyeok Kim, and Dong kun Noh. "Adaptive data aggregation and compression to improve energy utilization in solar-powered wireless sensor networks." *Sensors* 17, no. 6 (2017): 1226.
- [12] Muthukumaran K, Chitra K, and Selvakumar C. "An energy efficient clustering scheme using multilevel routing for wireless sensor network." *Computers & Electrical Engineering* 69 (2018): 642-652.
- [13] Haythem Hayouni, and Mohamed Hamdi. "A Data Aggregation Security Enhancing Scheme in WSNs Using Homomorphic Encryption." *Intelligent Automation & Soft Computing* (2017): 1-9.
- [14] Mohamed El Fissaoui, Abderrahim Beni-Hssane, and Mostafa Saadi. "Mobile Agent Protocol based energy aware data Aggregation for wireless sensor networks." *Procedia Computer Science* 113 (2017): 25-32.
- [15] E. G. Prathima, Venugopal K. R., S. S. Iyengar, and L. M. Patnaik. "SDACQ: Secure Data Aggregation for Coexisting Queries in Wireless Sensor Networks." *International Journal of Computer Science and Network Security (IJCSNS)* 17, no. 4 (2017): 205.

- [16] Dilip Kumar, Trilok C. Aseri, and R. B. Patel. "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks." *Computer Communications* 32, no. 4 (2009): 662-667.
- [17] Haiyong Bao, and Rongxing Lu. "A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance." *Peer-to-Peer Networking and Applications* 10, no. 1 (2017): 106-121.
- [18] Hanady M. Abdulsalam, Bader A. Ali, Anwar AlYatama, and Eman S. AlRoumi. "Deploying a LEACH data aggregation technique for air quality monitoring in wireless sensor network." *Procedia Computer Science* 34 (2014): 499-504.
- [19] Tarunpreet Bhatia, Simmi Kansal, Shivani Goel, and A. K. Verma. "A genetic algorithm based distance-aware routing protocol for wireless sensor networks." *Computers & Electrical Engineering* 56 (2016): 441-455.
- [20] Jack Kirton, Matthew Bradbury, and Arshad Jhumka. "Source location privacy-aware data aggregation scheduling for wireless sensor networks." In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 2200-2205. IEEE, 2017.
- [21] Jaspreet Singh, and Kartik Sharma. "Energy efficient AODV routing protocol for mobile Ad-hoc network." *International Journal of Engineering and Computer Science* 4, no. 9 (2015).
- [22] Avinash Rai, and Preetu Patel. "Secure Data Aggregation Technique for Wireless Sensor Networks using Iterative Filtering Algorithm." *International Journal of Applied Engineering Research* 13, no. 18 (2018): 13805-13811.
- [23] Khalid A. Darabkh, Noor J. Al-Maaitah, Iyad F. Jafar, and Ala'F Khalifeh. "EA-CRP: A novel energy-aware clustering and routing protocol in wireless sensor networks." *Computers & Electrical Engineering* (2017).
- [24] Khalid A. Darabkh, Saja M. Odetallah, Zouhair Al-qudah, Khalifeh Ala'F, and Mohammad M. Shurman. "Energy-Aware and Density-Based Clustering and Relaying Protocol (EA-DB-CRP) for gathering data in wireless sensor networks." *Applied Soft Computing* 80 (2019): 154-166.
- [25] Li Qing, Qingxin Zhu, and Mingwen Wang. "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks." *Computer communications* 29, no. 12 (2006): 2230-2237.
- [26] Maryam Sabet, and Hamidreza Naji. "An energy efficient multi-level route-aware clustering algorithm for wireless sensor networks: A self-organized approach." *Computers & Electrical Engineering* 56 (2016): 399-417.
- [27] Mohamed Elshrkawey, Samiha M. Elsherif, and M. Elsayed Wahed. "An enhancement approach for reducing the energy consumption in wireless sensor networks." *Journal of King Saud University-Computer and Information Sciences* 30, no. 2 (2018): 259-267.
- [28] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, and Sanjay Jha. "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks." *IEEE Transactions on Dependable and Secure Computing* 12, no. 1 (2014): 98-110.

- [29] Vimal Kumar, and Sanjay Madria. "Pip: Privacy and integrity preserving data aggregation in wireless sensor networks." In 2013 IEEE 32nd International Symposium on Reliable Distributed Systems, pp. 10-19. IEEE, 2013.
- [30] N. R. Wankhade, and Dr. D. N. Choudhari. "Novel energy efficient election based routing algorithm for wireless sensor network." *Procedia Computer Science* 79 (2016): 772-780.
- [31] Rongxing Lu, Kevin Heung, Arash Habibi Lashkari, and Ali A. Ghorbani. "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT." *IEEE Access* 5 (2017): 3302-3312.
- [32] Tao Yang, Xu Xiangyang, Li Peng, Li Tonghui, and Pan Leina. "A secure routing of wireless sensor networks based on trust evaluation model." *Procedia computer science* 131 (2018): 1156-1163.
- [33] Tianshu Wang, Gongxuan Zhang, Xichen Yang, and Ahmadreza Vajdi. "Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks." *Journal of Systems and Software* 146 (2018): 196-214.
- [34] Yuanzhu Peter, Chen, Arthur L. Liestman, and Jiangchuan Liu. "A hierarchical energy-efficient framework for data aggregation in wireless sensor networks." *IEEE Transactions on Vehicular Technology* 55, no. 3 (2006): 789-796.

Figures

Figure 1

Architecture of the Proposed Method

Figure 2

Flow diagram for different phases of the protocol proposed

Figure 3

MAC block diagram

Figure 4

Verification process

Figure 5

Performance analysis in terms energy consumption

Figure 6

Processing Time

Figure 7

Overall cluster performance

Figure 8

Throughput

Figure 9

Delay

Figure 10

Energy Consumption