Maximizing Network Lifetime using Fuzzy Based Secure Data Aggregation Protocol (FSDAP) in a Wireless Sensor Networks

Reshma S, Shaila K, Venugopal K R

Abstract*: *Abstract*: Secure Data Aggregation in Wireless Senor Networks (WSNs) is a challenging issue. The various protocols has been suggested in the recent past such as EDIT[13], ADA[8], TSDA[9], SEDAN[10]. These protocols effectively meet the constraints of WSNs. In this paper, we have proposed a Fuzzy Based Secure Data Aggregation protocol (FSDAP) which is an efficient localized protocol. The FSDAP protocol is designed with three phases. The first phase selects Aggregator Node using ANS algorithm. An ANS algorithm involves two steps to elect an Aggregator Node in the clustered network. In first step, the cluster head is selected based on the Euclidean distance and in second step, the cluster head is selected based on the fuzzy product and fuzzy value (α). Then, in second phase, a selected AN eliminates data redundancy sensed by all sensor nodes within the cluster. Finally, in third phase, the FSDAP protocol effectively detects malicious node and provides secure data transmission path. Thus, the proposed protocol, FSDAP utilizes the node's resource parameter uniformly, which in turn improves Network Lifetime, maximizes Throughput Rate, maximizes Packet Delivery Ratio and minimizes End-to-End Delay. The FSDAP is simulated using the NS2 simulator and compared with centroid algorithms Fuzzy C-Means and K-Means algorithm and a secure aggregation protocol implemented using SAR (Secure Aware Ad hoc Routing). The time complexity of FSDAP protocol is O(m2n).

Keywords: Data Aggregation, Data Transmission, Fuzzy, Malicious Node, Localized, Network Lifetime, Wireless Sensor Networks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of a large number of tiny sensor nodes and one or more base stations. The tiny sensor nodes are capable of sensing, processing and sending an event to the base station. The sensor nodes are battery powered and limited resource constrained devices.[1][2]. So, it is necessary for the WSNs applications to utilize the resource effectively.

WSNs have diverse applications viz., Disaster relief operations, Biodiversity mapping, Intelligent building[3], Health care[4], Machine Surveillance and Preventing Maintenance [5][6]. For example, the environmental conditions are measured using spatially distributed independent sensor nodes and can be accessed by the user as shown in Fig. 1. The real-world applications collect data from multiple sensor nodes. The sensor nodes sense redundant data and transmit to the base station. The redundant data transmission consume more energy[7] and depletion of more energy in the network results with network partition. Therefore, the practical solution is to aggregate the sensed data before data transmission. Hence, it is necessary to elect an efficient Aggregator Node (AN).

Fig. 1: Wireless Sensor Networks (WSNs) Infrastructure

There are various data aggregation protocols viz., Tree - Based, Cluster - Based and Hybrid Data aggregation[8][9] that are used to elect an efficient AN. In cluster-based data aggregation protocols[10][11][12], the aggregator node is elected based on distance and residual energy and EBRP[13] protocol elects the Aggregator Node (AN) based on energy density, residual energy and distance. Mahalanobis distance, membership value and Fuzzy C−Means algorithm to extract ellipses from the cluster are used in [14]. Thus, it covers the whole network and avoid holes in network and thus guarantees data delivery to the base station. The objective of the aggregation protocols is to minimize the redundant data transmission and maximizes Network Lifetime. The afore mentioned aggregation protocols minimize redundant data transmissions in network [15][16] and prolongs Network Lifetime. But various aggregation protocols efficiently do not meet the resource constraints.

In addition to data aggregation, it is also necessary to provide security for successful data delivery to the base station with effective utilization of available resource parameters. There are various security attacks [17] viz., snooping attack, worm hole attack, black hole attack, packet replication attack, Denial-of-Service (DoS) attack, Distributed DoS (DDoS) attack, etc. In this paper, the proposed protocol focuses on mitigating black hole attacks. Black hole attack is one kind of attack launched on the DSR or AODV routing protocol. DSR or AODV is an on-demand routing protocols where source node and destination node communicates by sending a route request (RREQ) and route reply packet (RREP) packet. When sender sends a route request (RREQ) packet to another node, the attacker listens to the request and returns a route reply (RREP) packet to the node that it has a shortest path to the base station. As a

Revised Manuscript Received on November 19, 2019.
***** Correspondence Author
Reshma S*, Department of Computer Science and Engineering, Visvesvaraiah Technological University-Research Resource Center, Belagavi, Karnataka, India, email-id: reshmam211@gmail.com
Shaila K, Professor and HOD, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru, Karnataka, India.
Venugopal K R, Vice Chancellor, Bengaluru University, Bengaluru, Karnataka, India.

result in black hole attack, malicious node uses spurious route updates to attract network traffic that is dropped later. Hence, to avoid black hole attack, it is necessary to identify id of legitimate node and malicious node.

There are various black hole detection methods for on-demand reactive routing protocols viz., Detection based on path based method[18], Detection based on collaborative Bayesian method[19], Detection based on learning automata[20], Detection using fuzzy logic[21], Detection using Anomaly Detection, Detection of cooperative black hole attack[22], MR-AODV[23], Detection using promiscuous node[24].

A. Motivation

The limited resource utilization is a major constraint in Wireless Sensor Networks. The redundant data transmission in the network depletes the node's energy and broadcasts packets through a spurious routing path which results in packet loss So, it is required to aggregate data and to identify legitimate node id before data transmission. Hence, it is essential to select an efficient aggregator node for data aggregation and secure path to guaranty delivery of the aggregated data to base station. There exists various secure data aggregation protocols but these protocol do not utilize the resources efficiently. Therefore, it is necessary to collaboratively elect the aggregator node and a legitimate node. In order to achieve this, it becomes essential to design and develop secure data aggregation routing protocols for data transmission so as to increase the network lifetime.

B. Contribution

The proposed protocol considers clustered network architecture in which the aggregator node for each cluster is elected based on two parameters (i) Euclidean distance and (ii) Fuzzy Distance. The fuzzy distance is computed using uzzy product and fuzzy value to identify the centroid position of the cluster and the node located in the centroid is onsidered as an aggregator node (AN). An aggregator node then scertain secure path by identifying legitimate node using Secret Key value. This protocol consumes less energy and utilizes energy uniformly across all nodes in the entire network resulting in maximizing *network lifetime*, aximizing *network throughput*,maximizing *packet delivery ratio* and minimizes *End-to-End Delay*.

C. Organization

The brief description of related works is presented in Section II and discusses the background work in Section III. Section IV defines the problem and objectives while Section V describes system and mathematical model along with proposed algorithm. Section VI presents the performance evaluation. The concluding remarks are summarized in section VII.

II. RELATED WORK

Various protocols related to secure data aggregation are discussed in this section.

Junchao et al., [25] designed a contiguous link scheduling protocol for data aggregation in WSNs. EDGE [26] tree is constructed to aggregate data and finds an interference free link for the sensor nodes to collect data with minimum number of time slots. EDGE tree gathers and aggregates the data. The sink node is embedded as root and data sensed by child node are forwarded to the sink through the intermediate parent node. Contiguous link scheduling allows nodes to be awakened only once and hence saves the battery life resulting in delay and possibility of data loss.

Shaila et al., [27] proposed an efficient Secured Quality of Service (QoS)-Aware Data Fusion (SQDF) for Wireless Sensor Networks. SQDF fuses the data at an intermediate node in a specific time interval and also detects the malicious nodes in four phases. Firstly, it broadcasts hello message to all the nodes in the network and then it waits for certain period of time which is required for data fusion. If the node utilizes the extra time over many transmission, then the node is considered as a malicious node and the same is reported to control center. The control center broadcasts this report to the whole network and it excludes the malicious nodes in the network. Thus, it reduces the packet loss and efficiently detects the malicious nodes in the network.

Ibrahim et al., [28] applies an energy efficient Tree - Based Data Aggregation approach in Wireless Sensor Networks using Fitting Function. Here, the local aggregation and prefix algorithms eliminate the similar data based on the difference of predefined threshold value and then fits these aggregated data with the equation for transmission. Thus, it saves energy by minimizing the data packets sent from the aggregator to the sink node. The equations used for accomplishing data with the fitting function results in communication overhead.

Zhou et al., [29] proposed Mixed Integer Programming to compute data gathering trees with different aggregation modes viz., full aggregator, non aggregator and hybrid aggregator in Wireless Sensor Networks. It improves the network lifetime, but increases the overhead of calculating the threshold value to validate the aggregator node.

Fengyuan et al., [30] proposed a scalable, adaptable and efficient Attribute-Aware Data Aggregation (ADA) scheme. This scheme uses a packet attribute that converges similar kind of sensors to one attribute; it assigns the natural number for identifying the packet attribute and there is a possibility of the number being hacked. Hence, a suitable computation number has to be generated for the packet attribute.

Yanbing et al., [31] presented a Trust Based Secure Data Aggregation (TBSDA) protocol for IoT. Secure data aggregation is achieved by behavior-detection, trust evaluation and data assembling technique. In TBSDA protocol, cluster head plays an important role in detecting the malicious nodes. Cluster head calculates trust weight and compares it with the average trust weight of the nodes in the cluster. This improves the network lifetime and reduces intra attacks like selfish attack.

Rabia et al., [32] developed an Adaptive Data Aggregation (ADA) protocol based on the correlation of the nodes. This protocol calculates ε (deviation of the difference between two messages) which produces less distortion, reduces the payload size and compression ratio. Overhead is increased since ε is calculated at each node.

Traditionally, the cluster heads are elected based on the residual energy of the cluster members in the clusters. This methodology

helps the adversaries to advertise the fake energy level and to drop the packets. Hence, it is necessary to strengthen the parameters which are used to elect the cluster head. Therefore, a fuzzy logic approach is used to elect the cluster head and provide security to the network. Finally, the elected cluster head sends the aggregated data to the base station.

Lazzerini et al., [33] presented a fuzzy approach to reduce the power consumption in Wireless Sensor Networks. Data Aggregation is done at each node based on the triangular fuzzy number and weighted average operators. This improves the energy efficiency because it aggregates data when two fuzzy numbers intersect with each other.

Jia et al., [34] presented an improved cluster routing protocol LEACH-KED based on the energy and distance. The cluster is distributed based on the k-means algorithm and then the cluster head is elected based on the weight value which is computed using the position information, residual energy and distance from the base station. Thus, it uniformly utilizes the nodes energy and improves the network lifetime

Ankit et al., [35] proposed an Energy Delay Index for Trade-off (EDIT) protocol to elect an efficient cluster head in the Wireless Sensor Networks. EDIT elects a cluster head based on the energy and distance between cluster head and the member node. The trade-off between energy and delay is determined by considering two different types of distance viz., Euclidean distance and hop-count. Thus reducing the delay and maximizing network lifetime.

Jeorge et al., [36] presents an Online-KISSME Stream algorithm that computes the path based on Mahalanobis distance matrix in an online way. It dynamically updates the Mahalanobis matrix and is used whenever source node detects an event. This algorithm utilizes extra energy for periodic update of Mahalanobis matrix.

Rezvani et al., [37] proposed an efficient improved Iterative Filtering (IF) algorithm in Wireless Sensor Network. This IF algorithm collects the data simultaneously from all the sensor nodes and aggregates it by averaging all sensor reading towards the lower weight and computes trustworthiness assessment to provide better security in the network.

Jiahu et al., [38] developed a distributed k-Means algorithm and fuzzy c-Means algorithm for Wireless Sensor Networks. In this protocol, the sensed data is partitioned based on the membership values assigned to each node and it computes the centroid of the cluster based on k-Means centroid algorithm and fuzzy c-Means algorithm. Further, it uses the consensus theory to elect the aggregator node based on the centroid and membership values. Finally, this algorithm promises data delivery to the base station with minimum energy utilization and increase in computation overhead.

Navjot et al., [39] proposed a Distance based Angular Clustering Algorithm (DACA) for WSNs. The DACA algorithm finds the path based on node's energy, distance and path energy. The calculation of path overhead arising from the data transmission of source node to base station is reduced. Thus, it utilizes energy uniformly in the networks which in turn improve network lifetime. This algorithm is prone to attract the intruder since an intruder can advertise minimum path energy and can elect the cluster head.

Chobe et al., [40] uses 2ACK scheme to detect misbehavior nodes in routing. This scheme includes 2ACK acknowledgement packet to acknowledge in the routing path between two hop node and source node. Thus guarantees the delivery of a data, minimizes latency and routing overhead.

Hesiri et al., [24] proposes solution to identify and prevent black hole attack in MANET. It includes Data Routing Information (DRI) table which maintains the node id of all the participated and non participated nodes, and Further REQ and Further REP packet to verify the intermediate nodes between source and destination. This helps to improve throughput rate and reduces packet loss. But too many REQ and REP packets lead to routing overhead.

Siddarth et al., [41] proposes a modified AODV routing protocol to detect and prevent black hole attack in MANET. AODV routing protocol updates the neighbor node id in the routing table of source node when it receive the reply from RREQ. This routes the packet to the node which is present at the first position in the source node's routing protocol. This helps the black hole node to advertise that it is having shortest path and to reply the RREQ. So the author modified this AODV protocol by sending the packet to the node which is present at second position in the routing table. Therefore, it reduces packet loss but increases latency and minimizes throughput rate.

Bhalaji et al., [42] analyzes the behavior of black hole attack in MANET and categorizes nodes based on the behavior of node. The source node identifies the trusted node based on the trust value and threshold value stored in the routing table. This protocol arranges the nodes in the routing table based on the trust value. The nodes which have highest trust value are stored at the first position in the routing protocol. Thus increasing the routing security and encourages node's cooperation. The trust value is assigned based on the experience of node.

Khulbhusan et al., [43] presented Fuzzy Logic based intrusion detection system against black hole attack on AODV in MANET. This Intrusion Detection System (IDS) detects the black hole attack using Fuzzy Logic and it raises an alarm. The neighbor nodes which hear an alarm updates the routing table with the malicious node id. It provides the better security in the network and minimizes the black hole attack. But this technique considers only fidelity level to verify the non promiscuous node.

Taylor et al., [44] proposes ADIOS to mitigate black hole attack. It uses the combination of watchdog mechanism and light weight expert system on each node. Watchdog monitors the nodes behavior in the network and light weight expert system is designed using Artificial Intelligence to detect malicious nodes in the network. This combination helps to detect and prevent malicious node but the malicious node id has not been maintained in the routing table. Hence, it repeats executing an algorithm if the same malicious node enters into the network.

Sonal et al., [45] proposed an algorithm to detect a black hole attack using fuzzy logic. Source node identifies the legitimate node based on the priority level. The priority level has been identified based

on packet loss and data rate. Thus, reducing data loss rate over the network.

Pnoonam et al., [46] presented an Intrusion Detection System (IDS) using fuzzy logic to detect a black hole attack. It finds the solution based on two factors viz., destination sequence number and data forwarding packet ratio during the response time of node's communication. This reduces the data loss over the network.

Gayatri et al., [47] suggested the mechanism for detecting and defending against a cooperative black hole attack. This mechanism uses two paradigm viz., Maintenance of Routing Information Table(RIT) and reliability checking of a node. Routing information table are updated with the bit value assigned for three cases viz., from node, a node and through trustful node. Reliable data transmission is performed based on this value and is stored in RIT. This helps to decrease routing overhead and end to end delay. But during the data transmission, if the next hop neighbors bit value of trustful node is 0 in the source node RIT considers the next hop neighbor node as malicious node even if that node is not a black hole node.

Neeraj et al., [48] detected and avoided worm hole attack and black hole attack. Nodes are categorized during the communication between the source node and destination node based on the node's cooperation and trust value viz., Unreliable, reliable and most reliable. The computed trust value are maintained in the routing table to help to detect the malicious node. This increases throughput, packet delivery ratio and utilizes less energy. But the trust value computed is based on throughput rate, and prone to black hole attack.

Fidel et al., [49] presents a trust based approach for AODV to mitigate black hole attack in MANET. The trust value is calculated based on the packet delivery ratio. So, when the node receives RREP message from neighbor node after broadcasting the RREQ, it verifies the node's trust value with the threshold (0.3). In turn improves packet delivery ratio.

All the above protocols use the parameters viz., energy, depth, Euclidian distance, fuzzy rule based on the packet delivery ratio, etc., to elect a cluster head and to detect the malicious nodes. But it is required to add more parameters to build a strong fuzzy rule. Thus, it helps to identify and to avoid non promiscuous node in WSNs. Hence, the proposed protocol considers *the fuzzy product, fuzzy value and consensus theory, residual energy and distance* to design a strong fuzzy rule. To mitigates the non promiscuous node attacks.

III. BACKGROUND

The existing secure data aggregation protocols are tradeoff between security and shortest path, causing uniform utilization of node's energy in the network. In order to overcome this problem the protocols - [50] is designed with the combination of centroid algorithms that are distributed K-Means algorithm and fuzzy C-Means algorithm, [51] is designed with SAR protocols. In K-Means and C-Means algorithm, the sensed data is partitioned based on the membership values assigned to each node and computes the centroid of the cluster. Further, it uses the consensus theory to elect the aggregator node based on the centroid and membership values. In SAR protocol, the author addressed two main security challenges in secure data aggregation *viz.*, confidentiality and data integrity. The SAR protocol mitigates black hole attack, worm hole attack and grey hole attack. This protocol increases average end-to-end delay time since this protocol is not focused on shortest path. It discovers route only with a 'quantifiable guarantee of security'. Finally, the centroid algorithms promises data delivery to the base station with minimum energy utilization and increase in computation overhead where as SAR protocols also guarantees the packet delivery with increased latency.

In our work, we have focused on both security and shortest path which computes centroid by electing the aggregator node based on the *fuzzy product, fuzzy value and consensus theory;* Secret Key using *energy and distance*. This protocol utilizes the energy uniformly, reduces computation overhead, decreases end-to end-delay, increases Network lifetime and maximizes throughput.

IV. PROBLEM DEFINITION

Consider *n*, *e* and *k* as number of nodes, remaining energy of a node and number of clusters in the network respectively. If *x*, a malicious node enters into the network, then assurance of packet delivery to the base station is difficult. Due to limited resource constraints in Wireless Sensor Networks (WSNs), guaranteeing packet delivery with minimum energy utilization is necessary. The redundant data transmission in the network depletes node's energy at the earliest. This partitions the network which results in more energy consumptions and thus reducing the network lifetime.

The main objective of the research work is to:

(i) Balance the energy utilization of nodes in the network.

(ii) Increase the number of packet received at the base station.

(iii) Improve the network lifetime.

Assumptions:

(i) Initially all the nodes in the network possess same energy level.

(ii) Sink posses more energy compared with all the nodes in the network.

V. SYSTEM AND MATHEMATICAL MODEL

In order to overcome the drawback of existing protocol, the efficient secure data aggregation path is selected based on resource parameters *viz.*, distance(d), energy, *fuzzy_{value(\alpha)}*, *fuzzy_{distance(f_d)}* etc. Finally, the aggregated data is forwarded securely to the base station. Therefore, proposed system architecture designed with five phases as depicted in Fig. 2. (i) Node Deployment Phase. (ii) Aggregator Node Selection Phase (iii) Data Aggregation Phase (iv) Secret Key Generation Phase (v) Data Processing Phase.

Lemma 1: Let S is a set of N sensor nodes then each Cluster $\sum_{i=1}^{M} C_i \subseteq S$

Proof: Consider S_1, S_2, S_3 .... S_N is a set *'S'* of *'N'* sensor nodes and C_1, C_2, $C_{3,...}C_M$ is a

set *'C'* clusters in the network. Each cluster is a set of *'P'* sensor nodes then, $C_i = S_1, S_2, S_3 \ldots S_P$ where $C_i = S_1, S_2, S_3 \ldots S_P$ are the sensor nodes and are subset of *'S'*.

A. Node Deployment Phase

In this phase, with the proof of Lemma 1, *N* sensor nodes are deployed in fixed infrastructure and are collaborated to form a cluster. The x-cordinator matrix of each sensor node S_i in the cluster is defined as

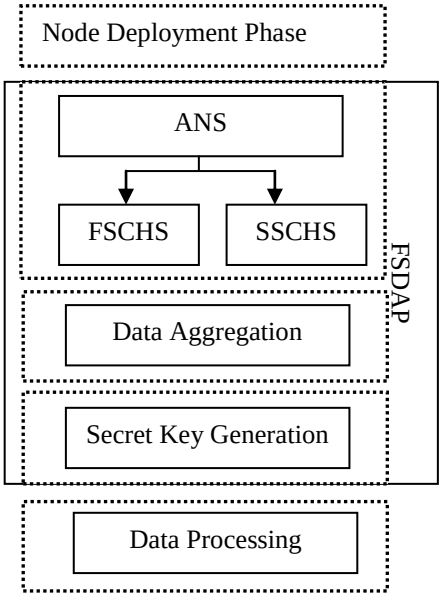

Fig. 2: Proposed System Architecture

$$x[j,i] = \begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} & \cdots & x_{1,P} \\ x_{2,1} & x_{2,2} & x_{2,3} & \cdots & x_{2,P} \\ x_{3,1} & x_{3,2} & x_{3,3} & \cdots & x_{3,P} \\ \vdots & & & & \\ x_{M,1} & x_{M,2} & x_{M,3} & \cdots & x_{M,P} \end{pmatrix}$$

The y-coordinator matrix of each sensor node S_i in the cluster is defined as

$$y[j,i] = \begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} & \cdots & y_{1,P} \\ y_{2,1} & y_{2,2} & y_{2,3} & \cdots & y_{2,P} \\ y_{3,1} & y_{3,2} & y_{3,3} & \cdots & y_{3,P} \\ \vdots & & & & \\ y_{M,1} & y_{M,2} & y_{M,3} & \cdots & y_{M,P} \end{pmatrix}$$

B. Aggregator Node Selection Phase

In this phase, data Aggregator Node (AN) is selected for aggregating the sensed data in each cluster and to transmit aggregated data towards base station. The selection is performed in two steps.

First Step Cluster Head Selection (FSCHS)

In this step, if the first event is generated then, the AN is selected based on shortest distance as in LEACH[16] protocol. Let *i = 1, 2, 3, ...N* nodes and *j = 1, 2, 3, ...M* clusters. The i^{th} node which is having the shortest path from its respective j^{th} cluster to the base station is considered as AN of j^{th} cluster. The shortest distance can be calculated using equation 1.

$$d(i,sink) = \sqrt{(x[s] - x[j,i])^2 + (y[s] - y[j,i])^2} \quad (1)$$

where, *i* ranges from *1, 2, 3, 4.....n, x[j, i]* is the *x* coordinate of node *i* in j^{th} cluster, *y[j, i]* is the *y* coordinate of node *i* in j^{th} cluster, *x[s]* is the *x* coordinate of node *s* and *y[s]* is the *y* coordinate of node *s*.

Second Step Cluster Head Selection (SSCHS)

If an event is second, third and so on, then the Aggregator Node (AN) is selected based on the centroid location of the cluster.

Lemma 2: If $Si \subseteq S$, then f_{diff} is a matrix of $\sum_{j=1}^{m}\sum_{i=1}^{n} x[i,j] - \mu$

Proof: Let $Si \subseteq S$ (discussed in Lemma1) *x[j, i]* is the x-coordinate of node $i \in C_j$ cluster and μ is the mean value calculated as shown in equation 2,

$$\mu = \frac{\sum_{j=1}^{m}\sum_{i=1}^{n} x[i,j] - \mu}{P} \quad (2)$$

The F_{diff} matrix gives the difference of sensor node's xcoordinate with the mean value to find the variance between the actual point and the mean point. The F_{diff} matrix is defined as

$$F_{diff} = \begin{pmatrix} x_{1,1} - \mu & x_{1,2} - \mu & x_{1,3} - \mu & \cdots & x_{1,P} - \mu \\ x_{2,1} - \mu & x_{2,2} - \mu & x_{2,3} - \mu & \cdots & x_{2,P} - \mu \\ x_{3,1} - \mu & x_{3,2} - \mu & x_{3,3} - \mu & \cdots & x_{3,P} - \mu \\ \vdots & & & & \\ x_{M,1} - \mu & x_{M,2} - \mu & x_{M,3} - \mu & \cdots & x_{M,P} - \mu \end{pmatrix}$$

Definition 1: FuzzyProduct (f_p)

It is given as square of product of fuzzy difference (F_{diff}) (proved in Lemma 2) and summation of transpose of fuzzy difference (F_{diff}).

The fuzzy product (f_p) is calculated using the equation 3,

$$F_p = \sqrt{(x[j,i] - \mu)^2 \sum (x[j,i] - \mu)^T} \quad (3)$$

where, *x[j, i]* is the *x* coordinate of i^{th} node in j^{th} cluster and μ is the mean value calculated as shown in equation 3.

Theorem 1:

$$F_p < \mu \Rightarrow F_p + \alpha, \quad (4)$$

$$\sim F_p < \mu \Rightarrow F_p + \alpha, \quad (5)$$

Proof: If the (f_p) value of i^{th} node is less than μ (in Equation 4), which mean that the centroid point is located little far away from the right side of the centroid point, so (f_p) is added with the α value point to a centroid of the circle. Similarly, if the (f_p) value of i^{th} node is greater than μ (in Equation 5) Fig. 3 shows that the centroid point is located little far away from the left. Hence, (f_p) value is subtracted from α to locate the centroid point. The α is calculated using equation 6.

$$\alpha = n\cos\frac{n}{m} \quad (6)$$

Example 1: In Fig. 4, given, *N* = 10, *M* = 2, *P* = 5, S = {*S1*,

S2, S3, S4, S5, S6, S7, S8, S9, S10}.

Step 1: With the proof of Lemma 1, consider the cluster *C1* = {*S1, S2, S3, S4, S5*} and *C2* = {*S6, S7, S8, S9, S10*}. In this example, lets discuss calculating centroid point for the cluster 1. The x-coordinate distance matrix of cluster *C1* is defined as

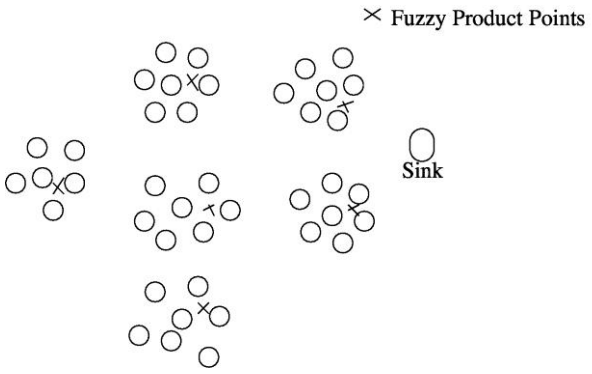

Fig. 3: Centroid Position of Clusters

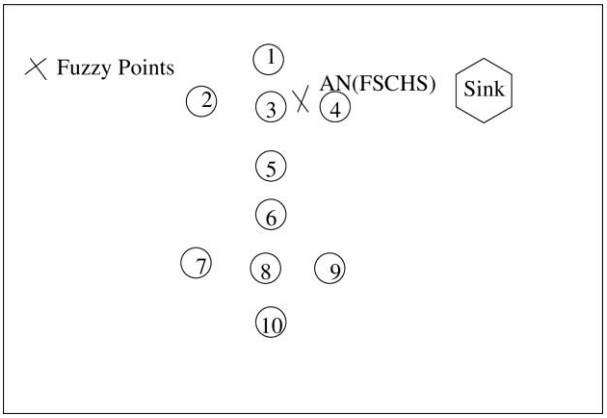

Fig. 4: Example1

$$x = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 2 \\ 3 \end{pmatrix}$$

Step 2: μ = 3.032,

Step 3: Compute F_{diff} using proof in Lemma 2 (see the equation 2). Therefore, the matrix of Fdiff is defined as

$$F_{diff} = \begin{pmatrix} 2.032 \\ 1.032 \\ 1.032 \\ 1.032 \\ 0.032 \end{pmatrix}$$

Step 4: Compute F_p using Equation 3.

$$F_p = 5.158$$

Step 5 : Compute α using equation 6.

$$\alpha = 2.84$$

Step 6: The F_p value computed in *Step 4* is greater than the μ value. Hence, as per the proof of theorem 1 (in Equation 5), the Fp value subtracts with the α value i.e., centroid point = 5.15 - 2.84 = 2.31.

Finally, the node situated at the centroid point in cluster 1 and nearest to the AN selected in FSCHS is elected as an AN.

In the Fig. 4, the node 3 is nearest to the *AN* selected in FSCHS and situated near to the centroid point, hence in cluster 1, the node 3 is considered as an AN.

The Example 1 illustrates the proof of Theorem 1. If the (F_p) value of i^{th} node is less than the mean distance (μ) from j^{th} cluster to the sink then, the α value is subtracted to locate the centroid (shown in equation 6). Therefore, the node which is situated at the centroid of the cluster is selected as an aggregaton node (AN) (see Equation 7).

$$AN = i \in \{F_p - \alpha\} \tag{7}$$

C. Data Aggregation

Consider *S1* and *S2* as a sensor nodes located in same cluster shown in Fig. 5. Nodes *S1* and *S2* senses data, and this sensed data is transmitted to an AN. The AN aggregates the redundant data, since redundant data transmission depletes node's energy soon.

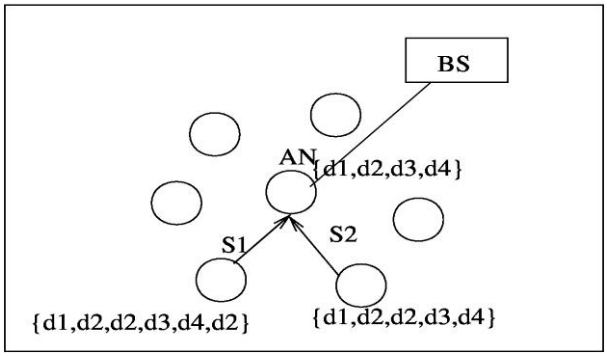

Fig. 5:Example2

Example 2: In Fig. 5, *S1 = {d1, d2, d2, d3, d4, d2}* and *S2 = {d1, d2, d2, d3, d4}* then an AN receives,

$$AN = S1 \cup S2 = \{d1, d2, d3, d4\}$$

D. Secret Ket Generation Phase

The secret key (*y*) value can be generated using an energy and distance parameters of a sensor node.

$$y = a1 + a0 \tag{8}$$

where *a1* and *a0* are the relationship value of energy and distance. The *a1* and *a0* is computed using the equation 9 and 10 respectively.

$$a1 = \frac{n * sumed * sume * sumd}{n * sumpe - sume^2} \tag{9}$$

$$a0 = \frac{sumd * sumpe - sume * sumed}{n * sumpe - sume^2} \tag{10}$$

Where

- *n* is the number of clusters in the network
- *sumed* is the product of distance and energy can be computed as

$$sumed = \sum_{i=1}^{N} \sum_{j=1}^{M} e_{ij} * d_{ij} \tag{11}$$

where e is the remaining energy of a node and D is the distance between AN and base station.

- *sume* is the summation of remaining energy of all nodes in the cluster,

$$sume = \sum_{i=1}^{N} \sum_{j=1}^{M} e_{ij} \quad (12)$$

- *sumd* is the summation of distance from the nodes in the cluster to base station,

$$sumd = \sum_{i=1}^{N} \sum_{j=1}^{M} d_{ij} \quad (13)$$

- *sumpe* is the summation of power of remaining energy of all nodes in the cluster,

$$sumpe = \sum_{i=1}^{N} \sum_{j=1}^{M} {e_{ij}}^2 \quad (14)$$

E. Data Processing Phase

The secret key, y is computed using equation 8 for all AN in the network. The routing table of AN consists of all node id, cluster id, Remaining Energy, Distance, AN id, AN's secretkey shown in Fig. 6. When an AN detects an event it is required to eliminate redundancy and should be transmitted securely to the base station. The AN verifies the secret key value advertises by an intermediate AN using the routing table information. If the computed secret key value and advertised secret key value of intermediate AN is same then the data is transmitted through that AN to the base station else it is considered as a non promiscuous node.

Node_Id	Cluster_Id	Remaining_Energy	Distance	AN_Id	AN's Secret Key

Fig. 6: Routing Tabe

F. Algorithm

The FSDAP algorithm for Secure Data Aggregation is shown in Algorithm 1 and Algorithm 2.

Algorithm 1: FSDAP Algorithm

```
Data: n - number of nodes, m - number of clusters
Result: Packet forwarding in an efficient path
Begin
step1: Broadcast "Hello" packet
step2: Generate an event
step3: First Step Cluster Head Selection
      for each event do
        if event = "first" then
          for k ← 1 to m do
            for i ← 0 to n do
              calculate d(i, sink)
            end for
          end for
          for k ← 1 to m do
            for i ← 0 to n do
              if i != "source node" then
                node ← c[k,i]
              end if
              if d[node, sink] < d[source node, sink] then
                min[k] ← d[node,sink]
                AN[k] ← node
              end if
            end for
          end for
        else
        for l ← 1 to m do
          for k ← 1 to m do
            for i ← 0 to n do
              node ← c[k,i]
              sum = sum + x[node]
            end for
          end for
          μ[l] = sum/m
        end for
        for k ← 1 to m do
          for i ← 0 to n do
            Compute fp =p(x[k, i] − x[μ])2(P(x[k, i] −
        x[μ])T
          end for
          Compute α = nlog(n/m)
        end for
        for k ← 1 to m do
          for i ← 0 to n do
            if d[i, sink] < mean[k] then
              avg ← fp + α
              AN[k] ← i
            else
              avg ← fp − α
              AN[k] ← i
            end if
          end for
        end for
      end if
    end for
step4: Secret Key Generation Algorithm
step5: Packet Forwarding from source to base station through
the aggregator node AN
End
```

Algorithm 2: Secret Key Generation algorithm

```
Begin
for k ← 1 to m do
        sume[k] ← 0
        sumpe[k] ← 0
        sumd[k] ← 0
        sumed ← 0
end for
for k ← 1 to m do
    for i ← 0 to n do
          for j ← 0 to n do
              sume[k] ← sumek[j]+energy[j]
              sumpe[k] ← sumpe[k]+energy[j]*energy[j]
              sumd[k] ← sumd[k]+ dist[j]*dist[j]
              sumed ← sumed + dist[j]*energy[j]
              denom ← m*sumpe[k]*sume[k]*sume[k]
               a0[k] ← (sumd[k]*sumpe[k]-
               sum[k]*sumed[k])/denom[k]
               a1[k] ←m*sumed[k]-sume[k] * sumd[k]) /
denom[k]
               y[k] ← a1[k]+a0[k]
          end for
      end for
end for
End
```

VII. SIMULATION AND PERFORMANCE EVALUATION

NS2 simulator is used to simulate FSDAP protocol. The FSDAP protocol is compared with Fuzzy C-Means[53] algorithm, K-Means[53] algorithm and SAR Protocol. Our simulation is set up for 50, 100 and 200 nodes respectively over the area of 1000*1000 meters. The sink node is located at 500m*500m and the simulation parameters are shown in Table I.

Table I. Simulation Parameter

Parameter	Values
Number of Nodes	########
Simulation Topology	500m * 500m
Traffic	CBR
Transmission Range	40m
Number of clusters	16
Initial energy	1J
Data packet size	64
Energy Consumed during Transmission	0.016J
Energy consumed during Receive	0.018J
Energy consumed during Idle	0.0005J
Simulation Time	20000 second

A. Performance Metric

Energy Utilization (EU): It is defined as the amount of energy utilized by all the nodes in the network for data aggregation.

Network Lifetime(NL): It is termed as maximum duration of fair network connectivity available for data transmission without partitioning the network.

Network Throughput (NT): It is the rate of total amount of packet received per unit time .

Packet Delivery Ratio: It is termed as the ratio of maximum number of packet delivered to the base station over number of packet sent.

End-to-End Delay: It is the time taken to deliver a packet from source node to the base station.

Time Complexity: It describes the amount of time taken to execute an algorithm.

B. Performance Evaluation

In our simulation, we considered 50, 100 and 200 set of sensor nodes and one sink node (shown in Fig. 7). The sensor nodes are collaborated to form a cluster and considered circle form of cluster architecture. Then AN for each cluster is elected based on the ANS algorithm. Each AN maintains a routing table as discussed in section V. In first iteration, event 1 is generated and forward to the base station through the AN elected in FSCHS and in second iteration, event 2 is generated and forwarded to the basestation through the AN elected in SSCHS.

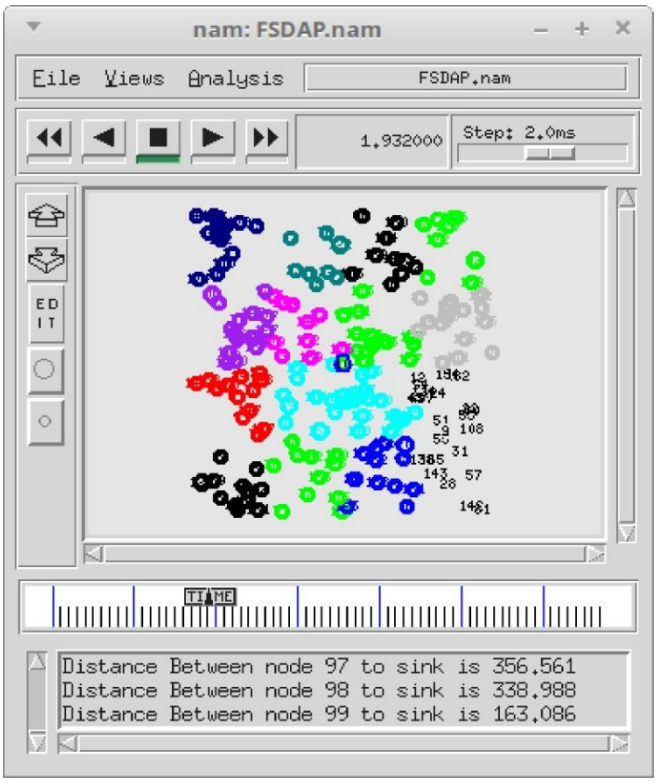

Fig. 7: Clustered Network

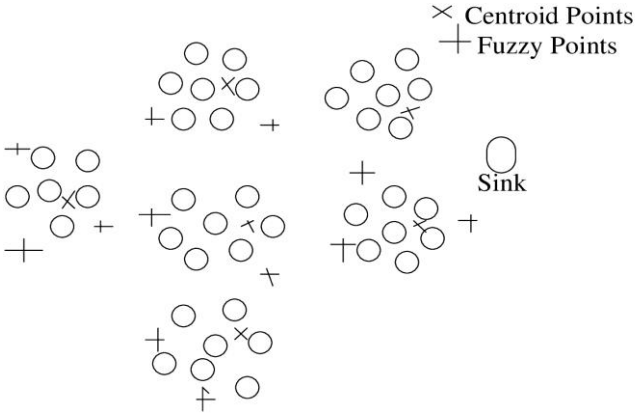

Fig. 8: Sample centroid calculated points

The two step procedure in ANS used to calculate centroid point. Since, in the SSCHS, centroid point is calculated based on the x-coordinate of sensor node. The node which is nearest to the AN is selected in FSCHS and to the centroid point is considered as an AN in the SSCHS.

In Fuzzy C-Means [50][53] algorithm, the centroid point cannot be obtained in a fixed iteration. It is observed in the Fig. 8 that '+' in the simulation result are the fuzzy points. It is calculated to find centroid of cluster using distributed Fuzzy C-Means and distributed K-Means algorithm. The cross '*' mark in Fig. 8 is the final centroid of cluster.

Fig. 9 shows the utilization of each node's energy for data transmission in the network and it is also observed that approximately all node's posess same energy level.

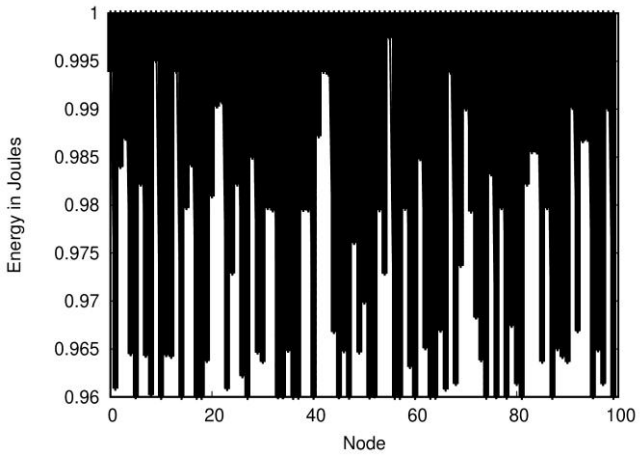

Fig.9: Energy Utilization of all the nodes in the cluster

Table. II: Network Lifetime

Simulation Time (Secs)	Energy in Joules			
	FSDAP	Fuzzy C Means [52]	K Means [52]	SAR [51]
2000	0.98	0.98	0.98	0.98
4000	0.98	0.98	0.98	0.97
6000	0.98	0.98	0.98	0.96
8000	0.97	0.94	0.96	0.92
10000	0.93	0.86	0.88	0.83
12000	0.92	0.83	0.85	0.79
14000	0.91	0.80	0.75	0.94

The fuzzy distance calculator computes the average distance to elect an aggregator node and it is reachable to all the node's in the cluster. This makes all node's to consume uniform energy for data transmission.

The analysis of Network Lifetime values for ANS, Fuzzy C-Means and K-means algorithm is shown in Table II. It is observed in the Fig. 11 that all three algorithm exhibit the same level of energy utilization till 6000s. The FSDAP protocol utilizes nodes energy uniformly by electing the cluster head based on the available resource in the network. Thus, the depletion of energy is slower compared with other two protocols. The Network Lifetime of FSDAP protocol implemented using ANS algorithm increase by 13% compared with Fuzzy C-Means algorithm and 18% over K-Means algorithm. Table II also shows the analysis of FSDAP and SAR Protocol. It is observed in Fig. 10, that the FSDAP protocol exhibits 17% increase in network lifetime when compared with SAR protocol.

The Aggregator Node Selection and Secret Key Generation phase in FSDAP protocol decreases the percentage of packet loss rate over data transmission. Fig. 12 shows the packet loss percentage over 50, 100 and 200 nodes when simulating FSDAP protocol. The ANS algorithm computes the average distance between the AN and all nodes in the cluster and secret key generation guarantees packet delivery by validating the generated secret key before data transmission. This prerequisite in the network increases throughput and decreases packet loss percentage. Fig. 13 shows the comparison between ANS, Fuzzy C-Means and K-Means based on packet loss percentage.

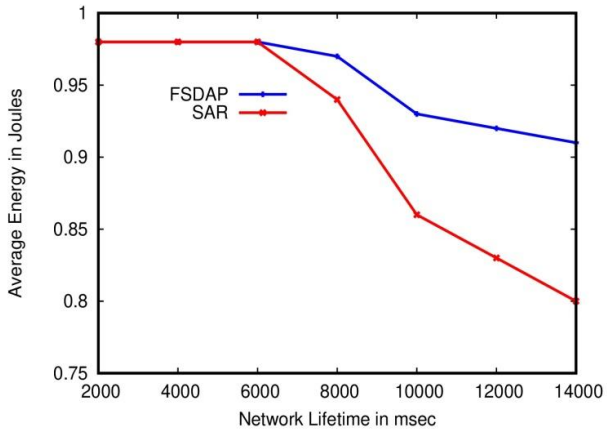

Fig. 10: NetworkLifetime Comparison with centroid algorithms

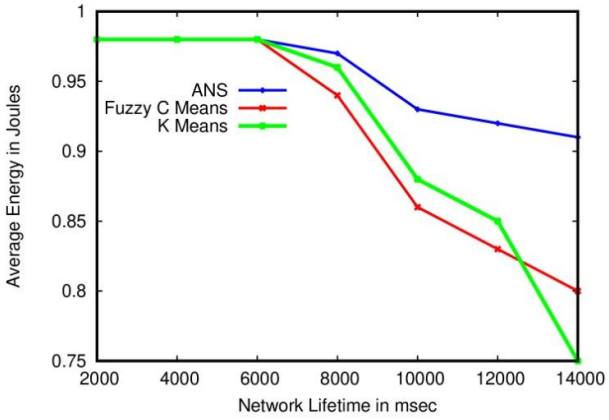

Fig. 11: NetworkLifetime Comparison with Protocols

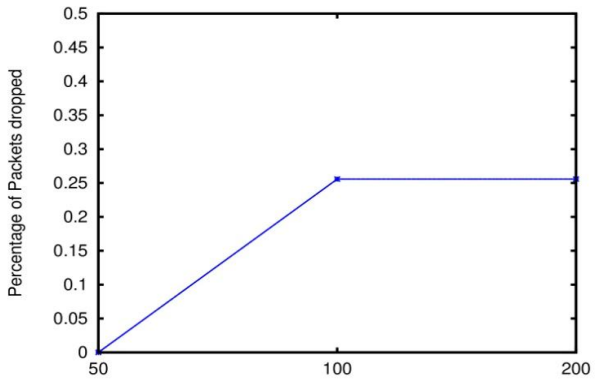

Fig. 12: Packet Loss

Table III shows the throughput rate of centroid algorithms iz., ANS, Fuzzy C-Means and K-Means algorithm and Secure Aggregation protocols viz., FSDAP and SAR. Fig. 14 shows illustrates the throughput rate in Kbps of ANS and other two

algorithms. The increased lifetime of the network improves the network connectivity. This guarantees the packet delivery between the source and the sink. Hence, ANS protocol exhibit better throughput rate compared with

Table. III: Network Throughput

Protocols		Packet Delivery	
	Throughput Rate	Number of Packets Sent	Number of Packets Received
FSDAP	0.996139	265	259
Fuzzy C-Means [52]	0.891294	265	225
K-Means [52]	0.853249	265	190

Table. IV: Time Complexity

Sl.No.	Number of Clusters	K-Means Time Complexity[52]	Fuzzy C-Means Time Complexity[52]	FSDAP Time Complexity
	n	$O(nmd)$	$O(m^2nd)$	$O(m^2n)$
1	1	300	300	100
2	2	600	1200	400
3	3	900	2700	900
4	4	1200	4800	1600
5	5	1500	7500	2500

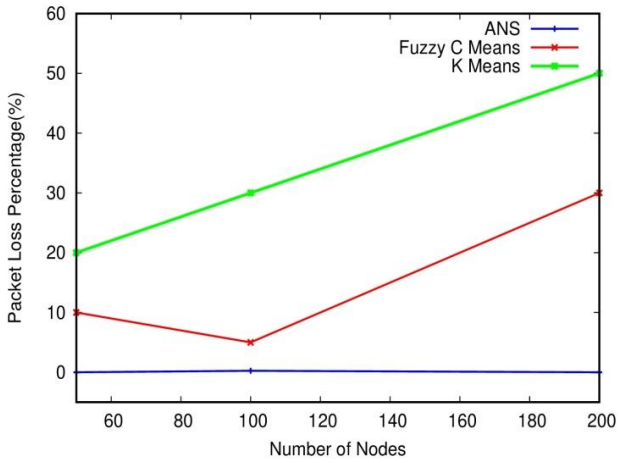

Fig. 13: Packet Loss Comparison with centroid algorithms

Fuzzy C-Means and K-Means algorithm. The throughput rate of ANS algorithm is increases by 11% compared with Fuzzy CMeans algorithm and 15% compared with K-Means algorithm.

Fig. 15 shows the throughput rate of FSDAP and SAR protocols. The SAR Protocol is a trade off between security and the shortest path, where as FSDAP protocol focuses on increased throughput rate. It is observed in Fig. 15 that FSDAP protocol increases throughput rate about 50%. Fig. 15 also discusses the comparison between FSDAP protocol using only ANS algorithm and FSADP protocol using ANS and Secret Key Generation Phase. Even when the inclusion of security the throughput rate of the network is improved.

Table III shows the number of packet delivered to the base station using ANS, Fuzzy C-Means and K-Means algorithm. The Fuzzy C-Means and K-Means algorithm iteratively executes to find the centroid of the cluster. Thus, makes the sensor node's to consume more energy and dies very quickly as depicts in Fig. 16 and Fig. 17. Fig. 16 shows that ANS possess 97% packets are delivered to the base station where as K-Means deliver 84% and Fuzzy C-Means deliver 71% of the packet to the base station respectively.

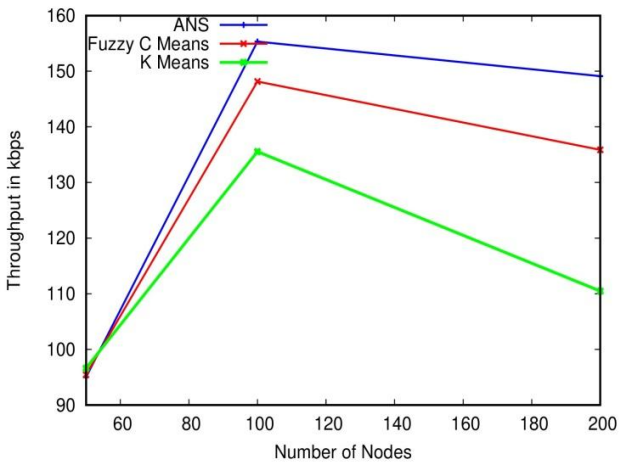

Fig. 14: Network Throughput Comparison with centroid algorithms

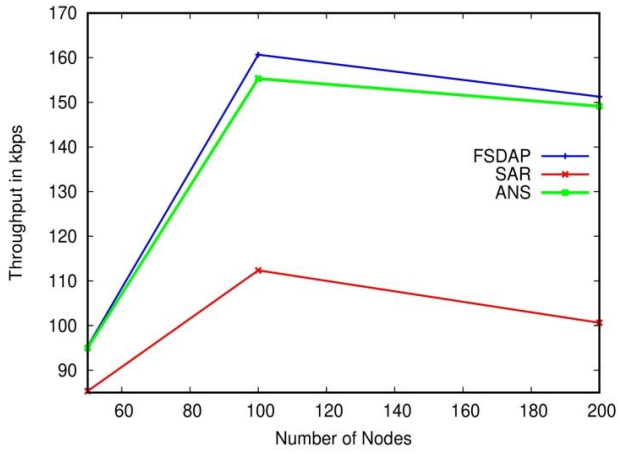

Fig. 15: Network Throughput Comparison with Protocols

The End-to-End Delay should be minimized in Wireless Sensor Networks (WSNs). Therefore, FSDAP protocols finds the average distance to

reach the destination to minimize the End-to-End delay.

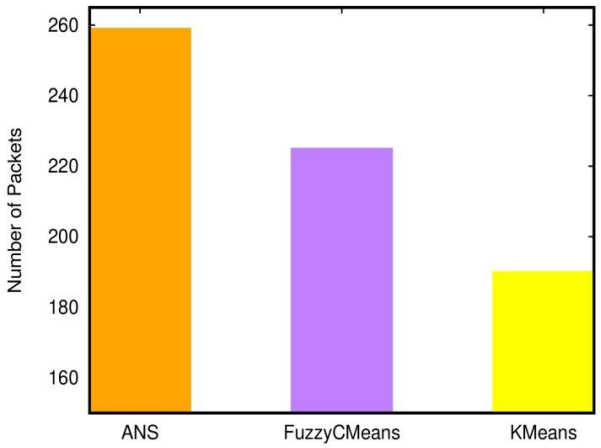

Fig. 16: Packet Delivery

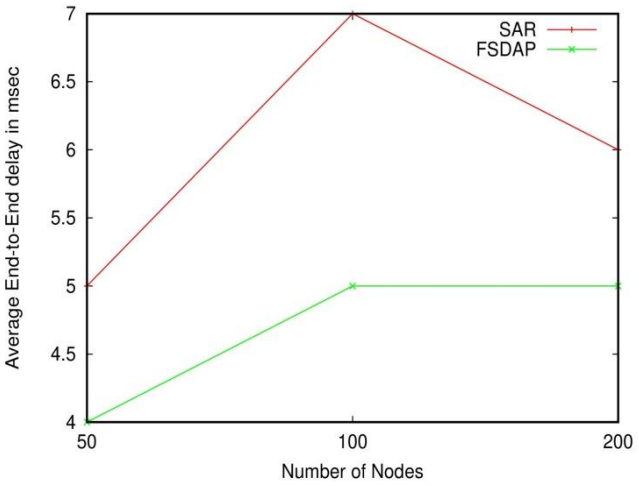

Fig. 17: End-to-End Delay

Fig. 17 shows the End-to-End delay of each packet from source to base station in FSDAP protocol and SAR protocol. The result reveals that FSDAP minimizes the packet delivery delay compared to Fuzzy C-Means and K-Means algorithm.

The simulation result in Table IV depicts the time complexity of the ANS algorithm, Fuzzy C-Means and K-Means algorithm for various clusters. Fig. 18 shows that ANS consumes 50% less time compared with Fuzzy C-Means and K-Means algorithm. But, if the number of cluster are more K means consumes 10% less time compared with ANS and Fuzzy C Means.

VIII. CONCLUSIONS

The redundant data transmission consumes more sensor node's energy. So, to utilize the node's energy efficiently and to eliminate the data redundancy, aggregating data. It is necessary to secure aggregated data in the network. The FSDAP protocol provides secure data aggregation using available resource parameters in the network. Firstly, select data aggregator nodes based on the available resource parameters *viz.*, Distance, Fuzzy product, Fuzzy value and Consensus Theory, then the AN aggregates the sensed data. Finally, the secret key value computed using residual energy and distance used to validate the non promiscuous node presence in the network. Simulation results shows the

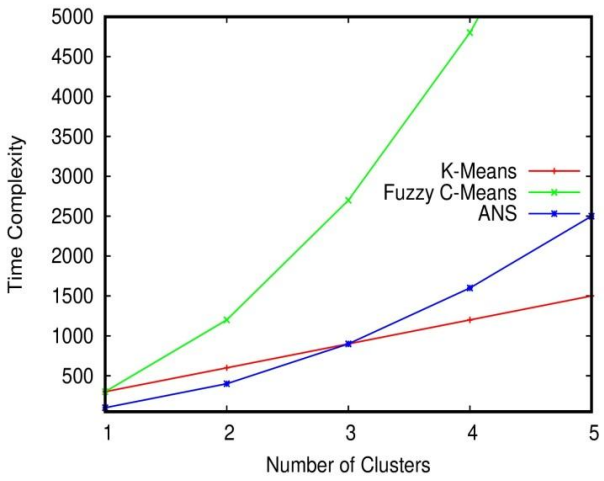

Fig. 18: Time Complexity

node's energy is utilized uniformly, Network Lifetime is maximize Packet Delivery Ratio and Throughput in the network.

REFERENCES

1. G Pottie and W Kaiser, "Wireless Integrated Network Sensors," *in Communications of the ACM*, 43(5), pp. 51-58, 2000.
2. Y Sang, H Shen, Y Inoguchi, Y Tan and N Xiong, "Secure Data Aggregation in Wireless Sensor Networks: A Survey," *in Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '06). IEEE Computer Society*, 43(5):315-320, 2006.
3. M Tubaishat, P Zhuang, Q Qi and Y Shang "Wireless Sensor Networks in Intelligent Transportation Systems," *in Transactions on Wireless Communications and Mobile Computing*, vol. 9, no. 3, pp. 287-302, 2009.
4. D Musiani, K Lin, and T S Rosing, "Active Sensing Platform for Wireless Structural Health Monitoring," *in Proceedings of the Sixth International Conference on Information Processing in Sensor Networks (IPSN '07). New York, NY, USA: ACM*, pp. 390-399, 2007.
5. S. Aeron, V. Saligrama and D. A. Castanon, "Efficient Sensor Management Policies for Distributed Target Tracking in Multihop Sensor Networks," *IEEE Transactions Signal Processing*, vol. 56,no. 6,p.2562-2574, June 2008.
6. A Milen Kovik, C Otto and E Jovanov, "Wireless Sensor Networks for Personal Health Monitoring: Issues and Implementation," *in Computer Communications*, vol. 29,no. 13,pp. 2521-2533, 2006.
7. Jia Guo and Xuemin Chen, "Survey on Secure Data Aggregation for Wireless Sensor Networks," *in Proceedings of IEEE International Conference on Service Operations, Logistics, and Informatics (SOLI)*, pp. 138-143, 2011.
8. Sandeep Kaur and R.C. Gangwar, "A Study of Tree Based Data Aggregation Techniques for WSNs," *in International Journal of Database Theory and Application* vol. 9,no. 1, pp. 109-118, 2016.
9. Mohammad Abdus Salam and Tanjima Ferdous, "Tree-based Data Aggregation Algorithms in Wireless Sensor Networks: A Survey," *in Proceedings of the 2012 International Conference on Industrial Engineering and Operations Management Istanbul, Turkey*, pp.1995-2002, 2012.
10. H AJzaid, E Foo, and G Nieto, "Secure Data Aggregation in Wireless Sensor Network: A Survey," *in Proceedings of the Sixth Australian Conference on Information Security (AISC '08)*, pp. 93-105, 2008.
11. S Ozdemir and Y Xiao, "Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview" *in Communication Networks* vol. 53,no. 12,pp. 2022-2037, March 2009.
12. V Kumar and S Madria, "Secure Data Aggregation in Wireless Sensor Networks," *in Proceedings of WSN Technologies for the Information Explosion*, pp.77-107, 2010.
13. B M Thippeswamy, Reshma S, Shaila K, Venugopal K R, S S Iyengar, L M Patnaik, "EDOCR: Energy Density On-Demand Cluster Routing In Wireless Sensor Networks," *in International Journal of Computer Networks and Communications (IJCNC),*

vol. 16, no. 1, pp. 223-240, 2014.
14. Hanane Barrah and Abdeljabbar Cherkaoui, "A Stabilizer Mahalanobis Distance Applied to Ellipses Extraction using the Fuzzy Clustering," *in Proceedings of International Conference on Multimedia Computing and Systems (ICMCS),* pp. 1059 - 1064, 2014.
15. R Roman, C Fernandez-Gao, J Lopez and H H Chen, "Trust and Reputation Systems for Wireless Sensor Networks" *in Security and Privacy in Mobile and Wireless Networking, S Gritzalis, T karygiannis and C Kianis, eds., Leicester, U K Troubador Publishing Ltd.,* pp. 105- 228, 2009.
16. Kiran Maraiya, Kamal Kant and Nitin Gupta, "Contiguous Link Scheduling for Data Aggregation in Wireless Sensor Networks," *in IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no. 7, pp. 1691-1701, July 2014.
17. I Rubin, A Behzad, R Zhang, H Luo and E Caballero, "TBONE: A Mobile-Backbone Protocol for Ad Hoc Wireless Networks," *in IEEE Conference on National Science Foundation,* pp. 2727-2740, 2002.
18. Abderrahmane Baadache and Ali Belmehdi, "Avoiding Black Hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," *in International Journal of Computer Science and Information Security (IJCSIS),* vol. 7, no. 1, pp. 10-16, 2010.
19. S Marti, T J Giuli, K Lai and M Baker "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," *in Proceedings of the Sixth Aannual International Conference on Mobile Computing and Networking,* pp. 255-265, 2000.
20. Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole Attack in Mobile ADHOC Networks," *in International Journal of Computer Applications (0975 - 8887),* vol. 1, no. 22, pp.38-42, 2010.
21. K Liu, J Deng, P K Varshney and Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," *IEEE Transactions On Mobile Computing,* vol. 6,no. 5, pp. 536-550, May 2007.
22. H Deng, W Li and D P Agarwal, "Routing Security in Wireless AdHoc Networks," *in IEEE Communications Magazine,* pp. 70-75, 2002.
23. S Ramaswamy, H Fu, M Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks," *in Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008,* pp. 22-24, 2008 .
24. H Weerasinghe and H Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation," *in Proceedings of IEEE Future Generation Communication and Networking (FGCN 2007)* pp. 362-367, 2007.
25.] Juncha Ma, Wei Lu and Xiang-Yang Li, "Design Guidelines for Maximizing Lifetime and Avoiding Energy Holes in Sensor Networks with Uniform Distribution and Uniform Reporting," *Proceedings IEEE INFOCOM,* pp. 1-10, 2006.
26. N Thepvilojanapong, Y Tobe and K Sezaki, "On the Construction of Efficient Data Gathering Tree in Wireless Sensor Networks," *in Proceedings of IEEE International Symposium on Circuits and Systems,* pp. 648-651, 2005.
27. Shaila K, Nalini L, Tejaswi V, Thriveni J, Venugopal K R and L M Patnaik, "Secure QoS Aware Data Fusion to Prevent Node Misbehavior in Wireless Sensor Networks," *in International Journal of Computer Science and Network Security (IJCSNS),* vol. 11, no. 3, pp. 31-40, March 2011.
28. Ibrahim Atoui;Ali Ahmad;Maguy Medlej;Abdallah Makhoul;Samar Tawbe;Abbas Hijazi, "Tree-Based Data Aggregation Approach in Wireless Sensor Network Using Fitting Functions," *in Proceedings of Sixth International Conference on Digital Information Processing and Communications (ICDIPC),* [17] pp. 146-150, 2016.DOI:10. 1109/ICDIPC.2016.7470808.
29. Fen Zhou,Zhenzhong Chen,Song GuoandJie Li, "Maximizing Lifetime of Data-Gathering Trees with Different Aggregation Modes in WSNs," *in IEEE Transactions Sensors Journal,* vol. 16, no. 22, pp. 8167-8177, Nov. 2016.
30. Fengyuan Ren, Jiao Zhang, Yongwei Wu, Tao He, Canfeng Chen and Chuang Lin, "Attribute-Aware Data Aggregation using Potential-Based Dynamic Routing in Wireless Sensor Networks," *in IEEE Transactions on Parallel and Distributed Systems,* vol. 24,no. 5,pp. 881-892, May 2013.
31. Yanbing Liu, Xuchong Gong and Congcong Xing, "A Novel Trust Based Secure Data Aggregation for Internet of Things," *in Proceedings of the Ninth International Conference on Computer Science and Education (ICCSE 2014),* pp. 435-439, August 2014.
32. Rabia Noor Enam and Rehan Qureshi, "An Adaptive Data Aggregation Technique for Dynamic Cluster based Wireless Sensor Networks," *in Proceedings of International Conference on Computer Communication and Networks (ICCCN),* ISSN: 1095-2055, pp. 33-38, 2014.
33. Beatrice Lazzerini,Francesco Marcelloni,Massimo Vecchio,Silvio Croce and Emmanuele Monaldi, "Using Mobile Relays to Prolong the Lifetime of Wireless Sensor Networks," *in Proceedings of Fuzzy Information Processing Society (NAFIPS),* pp.436-441, 2006. DOI:10.1109/NAFIPS.2006.3654 49.
34. Jia Yunjie,Liu Ming, Zhu Song and Dong Pengtao, "A Clustering Routing Algorithm Based on Energy and Distance in WSN," *in Proceedings of International Conference on Computer Distributed Control and Intelligent Environmental Monitoring,* pp. 9-12, 2012.DOI:10.1109/CDCIEM.2012.10.
35. Ankit Thakkar and Ketan Kotecha, "Cluster Head Election for Energy and Delay Constraint Applications of Wireless Sensor Network," *in IEEE Transactions on Sensors Journal,* vol. 14, no. 8, pp. 2658-2664, 2014. DOI:10.1109/JSEN.2014.2312549.
36. Jorge Luis Rivero Perez, Bernardete Ribeiro and Carlos Morell Perez, Mahalanobis Distance Metric Learning Algorithm for Instance-based Data Stream Classification," *in International Joint Conference on Neural Networks (IJCNN),* pp. 1857-1862, 2016.
37. Mohsen Rezvani, Aleksandar Ignjatovic, Sanjay Jha and Elisa Bertino, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," *in IEEE Transactions on Dependable and Secure Computing,* vol. 12, no. 1, pp. 98-110, January 2015.
38. Jiahu Qin, Weiming Fu, Huijun Gao, and Wei Xing Zheng, "Distributed k-Means Algorithm and Fuzzy c-Means Algorithm for Sensor Networks Based on Multiagent Consensus Theory," *in IEEE Transactions On Cybernetics,* vol. 47, no. 3, pp. 772-783, 2017.
39. Navjot Kumar and Surinder Kaur, "Distance based Angular Clustering Algorithm (DACA) for Heterogeneous Wireless Sensor Networks," *in IEEE Symposium on Colossal Data Analysis and Networking (CDAN),* pp. 1-5, 2016.
40. S N Chobe and Deepavali Gothawal, "An Acknowledgement Based Approach for Routing Misbehavior Detection in MANET with AOMDV," *in International Journal of Advanced Computational Engineering and Networking,* vol. 1, no. 5, pp. 5-10, 2013.
41. Siddharth Dhama, Sandeep Sharma and Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks," *in Proceedings of 3rd International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 279-284, 2016.
42. N Bhalaji and A Shanmugam, "Association Between Nodes to Combat Black Hole Attack in DSR Based MANET" *in Proceedings of IFIP International Conference on Wireless and Optical Communications Networks,* pp. 1-5, April 2009.
43. Kulbhushan and Jagpreet Singh, "Fuzzy Logic based Intrusion Detection System Against Blackhole Attack on AODV in MANET," *in International Journal of Computer Application,* NSC vol. 1, no. 2, pp. 28-35, 2010.
44. V F Taylor and Daniel T. Fokum, "Mitigating Black Hole Attacks in Wireless Sensor Networks Using Node-Resident Expert Systems," *in Wireless Telecommunications Symposium,* pp. 1-7, 2014.
45. Sonal and Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic," *in International Journal of Science and Research (IJSR),* vol. 2, no. 8, pp. 22-225, 2013.
46. Poonam Yadav, Rakesh Kumar Gill and Naveen Kumar, "A Fuzzy Based Approach to Detect Black hole Attack" *in International Journal of Soft Computing and Engineering (IJSCE),* vol. 2, no. 3, pp. 388-391, 2012.
47. Gayatri Wahane and Savita Lonare, "Technique for Detection of Cooperative Black Hole Attack in MANET," *in IEEE International Conference on Computational Intelligence and Computing Research,* pp. 1-6, 2014.
48. Neeraj Arya, Upendra singh and Sushma Singh, "Black Hole Attack Detection using Fuzzy Logic," *in IEEE International Conference on Computer, Communication and Control (IC4-2015),* pp. 1-5, 2015.
49. Fidel Thachil and K C Shet, "A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET" *in Proceedings of International Conference on Computing Sciences,* pp. 281-285, 2012.
50. Jiahu Qin, Weiming Fu, Huijun Gao and Wei Xing Zheng, "Distributed k-Means Algorithm and Fuzzy c-Means Algorithm for Sensor Networks Based on Multiagent Consensus Theory," *in IEEE Transactions on Cybernetics,* vol. 47, no. 3, pp. 772-783, 2017.
51. S Archana and A Saravana Salvan, "SAR Protocol Based Secure Data Aggregation in Wireless Sensor Networks," *in Proceedings of Ninth International Conference on*

Intelligent Systems and Control (ISCO) pp. 1-6, 2015.
52. Zeynel Cebeci, Figen Yildiz, "Comparison of K-Means and Fuzzy CMeans Algorithms on Different Cluster Structures," *in International Journal of Agricultural Informatics*, vol. 6, no. 3, pp. 13-23, 2015.
53. Soumi Ghosh and Sanjay Kumar Dubey, "Comparative Analysis of KMeans and Fuzzy C-Means Algorithms" *in International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 4, no. 4, pp. 35-39, 2013.

AUTHORS PROFILE

Reshma S, Research Scholar, Visvesvaraiah Technological University – Research Resource Center.
She is presently working as a Test Engineer in Evry India Pvt Ltd., Bangaluru. She received her Bachelors degree in Computer Science and Engineering from Visvesvaraya Technological University and Master of Technology from Visvesvaraya Technological University, Regional Center, Bangalore. Her research interest is in the area of Wireless Sensor Networks.

Dr. Shaila K, Professor in Department of Electronics and Communication and was the Head of the Department, Vivekananda Institute of Technology. She obtained her Ph. D in Computer Science and Engineering from Bangalore University, M.E in Electronics and Communication from University Visvesvaraiah College of Engineering, Bangalore University and B.E from PES Institute of Technology, Bangalore University, Bangalore. She has over twenty years of teaching experience. She has authored Digital Circuits and Systems published by Tata McGraw Hill, New Delhi and Secure Data Communication Techniques by LAP LAMBERT publishers, Germany.
She has published papers in refereed International Journals and International Conferences. She has received Best Teacher and Best Researcher Award. Her name appears in Marquis Who's Who in the World Science and Engineering. She is the Life member of ISTE, iMAPs, Member of ACM, IEANG and reviewer for conference and journals. Her research areas include Wireless Sensor Networks, Adhoc Networks and Image Processing..

Dr. Venugopal K. R., Vice Chancellor, Bangalore University. He has Eleven Degrees with Ph.D. in Computer Science Engineering from IIT-Madras, Chennai and another Ph.D. in Economics from Bangalore University. He has degrees in Law, Mass Communication, Electronics, Economics, Business Finance, Computer Science, Public Relations and Industrial Relations. He has authored and edited 64 books and published more than 700 papers in refereed International Journals and International Conferences. He has supervised 630 M.E. dissertations, 25 Ph.Ds and filed 101 Patents. He was a Post Doctoral Research Scholar and a visiting Professor at University of Southern California, USA. He has been conferred Fellow of IEEE, USA and ACM Distinguished Educator for contributions to Computer Science Engineering and Electrical Engineering Education.