Master Thesis

Master's Program in Network Forensics, 60 credits

A Method to Improve the Security of Information Diffusion in Complex Networks— Node Trust Value Management Mechanism

Halmstad 2020-05-31

Rahul Lal Radhakrishnan

HALMSTAD UNIVERSITY

Abstract

In a sensing field-based placement of nodes the communication happens from the data acquisition points to the control center which is the receiver of data acquisition. In this project an algorithm based on data sense points trust value updating is used which will find out the value of the trust level dynamically once the trust level is found out it will pick the forwarded data sense points based on highest value of trust. The NTTUA algorithm is then compared with baysian trust method and then pick the path which has the highest baysian trust. The comparison between NTTUA and baysian method is done with respect to multiple parameters which give good performance and better residual energy along with throughput.

Acknowledgments

I would like to thank our families for all the support, both financially and emotionally, throughout out studies. also appreciate it a lot for the instructions and help from Assoc. Professor Stefan Axelsson who is the mentor and examiner of this thesis. I would also like to thank our advisor, Wojciech Mostowski, for helping me with the thesis and giving us feedback regarding our work. Lastly, we are grateful to our teachers and fellow students for making this school year a great learning experience.

Table of Contents

Table of Figures 5

Table of Tables 7

Chapter 1: Overview of Wireless Sensor Network 8

1.1 Data Sense Points 8
1.2 Data Sense Area 8
1.2.1 Single Area Deployment 9
1.2.2 Multi Area Network 9
1.3 Previous Approach 11
1.4 Organization of the Work 12
1.5 Summary for the Work 12

Chapter 2: Methodology 13

2.1 Research Goals and Objectives 13
2.2 Project Flow 13
2.3 Comparison Parameters 14
2.4 Research Questions 15
2.5 Sensing Point Placement Strategy 17
2.6 Mathematical Model for DSPs Placement 21
2.7 Energy Utilization Process 22
2.8 Distance Communication Set 26
2.9 Classification of Efficient and Non-Efficient Set Analysis 28
2.10 Summary 31

Chapter 3: Literature survey 32

3.1 WSN 32
3.2 Energy Consumption 33
3.3 Lifetime Value Computation 35
3.4 Trust Level Computation 36
3.5 Summary

Chapter 4: Software Requirement Specification 37

4.1 Functional Requirements 38
4.2 Software and Hardware Requirements 39
4.3 High level design 39
4.4 Detailed design 42

Chapter 5: Implementation 48

5.1 Functions BAYSIAN Approach 51
5.2 Function Proposed Approach 58

Chapter 6: Testing **63**

6.1 Unit Test Cases 63

Chapter 7: Results **69**

7.1 Detailed Results Explanation 69

Chapter 8: Conclusion and Future scope **97**

8.1 Conclusion 97

8.2 Future Scope 97

8.3 Contribution 97

Chapter 9: Bibliography **99**

Table of Figures

Figure 1: Single Area Sensing Field……. 9

Figure 2: Homogenous Sensing Field…… 10

Figure 3: Non-Homogenous Sensing Field…… ... 11

Figure 4: Project Flow…….…….. 13

Figure 5: Initial Location for DSPs…..…….. 17

Figure 6: DSPs Location for Iteration1 …..…….. 18

Figure 7: DSP Location for Iteration2……..... 19

Figure 8: Location Changes for all DSPs…… 20

Figure 9: Mathematical Model for DSP Placement…… 22

Figure 10: Energy Consumption Model…… 23

Figure 11: Energy Consumption Distance …….…… 25

Figure12: Distance Computation between DSPs……... 27

Figure13: Efficient and Non-Efficient DSPs criteria …… 28

Figure14: Toolboxes……... 37

Figure 15: DFD Level1……. 39

Figure 16: DFD Level2……. 40

Figure17: DFD Level3…….. 41

Figure 18: DSP Placement Algorithm…….....43

Figure 19: Baysian Trust Method…… 44

Figure 20: NTTUA Method……46

Figure 21: Use Case Diagram ……48

Figure 22: Baysian Trust Method Function Diagram……..…51

Figure 23: NTTUA Method Function Diagram …… .58

Figure 24: Battery Initialization for the Nodes……70

Figure 25: Data Sense Points Distribution Algorithm……..71

Figure 26: Trust Level……..71

Figure 27: Number of Neighbors……..72

Figure 28: Path1 from IDSP to DDSP……72

Figure 29: Path 16 from IDSP to DDSP…..……73

Figure 30: Path1 from the IDSP 30 to DDSP 76……73

Figure 31: Route 16 from IDSP to DDSP ……74

Figure 32: Hops Measure……74

Figure 33: Trust Level Measure……..75

Figure 34: Paths v/s Trust Levels……..75

Figure 35: Best Route No……76

Figure 36: Residual Battery Energy for the Nodes……76

Figure 37: Battery Initialization for the DSPs.……...77

Figure 38: Data Sense Points Strategy Placement……..……77

Figure 39: Trust Level Initialization……...78

Figure 40: RREQ/RRLY for the Path1……..,78

Figure 41: RREQ/RRLY for the Path13…….....79

Figure 42: Path1 between IDSP to DDSP……79

Figure 43: Path13 IDSP to DDSP…….80

Figure 44: Best Route Discovered between initiator node to destination node……80

Figure 45: Route No versus Trust Level ……..81

Figure 46: Best Route Number v/s Trust Level……..,81

Figure 47: Remaining Battery Levels for the Nodes……82

Figure 48: Battery Initialization for the Network…….,82

Figure 49: Data Sense Points Placement Strategy……82

Figure 50: Comparison of Hops……83

Figure 51: Energy Consumption Comparison……...83

Figure 52: Number of Efficient DSPs……..86

Figure 53: Number of In-Efficient DSPs ……..…...86

Figure 54: Lifetime Ratio……87

Figure 55: Residual Energy Comparison……88

Figure 56: Overhead Comparison……..89

Figure 57: Throughput……89

Figure58: Node Deployment Algorithm…….91

Figure59: Energy Consumed Comparison……..92

Figure 60: Dead Nodes Comparison……93

Figure61: Routing Overhead Comparison……94

Figure 62: Throughput Comparison…….95

Figure63: Residual Energy Comparison……..96

Table of Tables

Table1 Location for DSPs 20
Table 2 DSP Locations 22
Table 3 Classical Energy utilization values 24
Table4 DSP1 distance with respect to other DSPs 26
Table 5 Initial Battery Energy 28

Table6 Distance between Detection points 29
Table7 Energy Utilization Value for DSP link 29
Table 8 Residual Energy after iteration 1 of path establishment for DSPs 30

Table 9 Residual Energy after 100 iterations of path establishment 30

Table10 Definition of Network Lifetime 35

Table 11: Functional Requirements 38

Table 12: Software and Hardware Requirements 39
Table 13: Functions Baysian approach 52-55
Table 14: Function Diagram for NTTUA method 57-61

Table 15: DSP Deployment Algorithm 63
Table 16: Distance Table Generation Test 63

Table 17: Path Discovery Algorithm BAYSIAN METHOD 64

Table 18: Path Discovery Algorithm NTTUA METHOD 64

Table 19: Comparison with BAYSIAN METHOD and NTTUA METHOD – End to End Delay 65
Table 20: Comparison with BAYSIAN METHOD and NTTUA METHOD – Number of Hops 65

Table 21: Comparison with BAYSIAN METHOD and NTTUA METHOD – Total Energy Consumption 66

Table 22: Comparison with BAYSIAN METHOD and NTTUA METHOD – Number of Efficient Nodes 66

Table 23: Comparison with BAYSIAN METHOD and NTTUA METHOD – Number of Dead Nodes 67

Table 24: Comparison with BAYSIAN METHOD and NTTUA METHOD – Routing Overhead 67

Table 25: Comparison with BAYSIAN METHOD and NTTUA METHOD – Lifetime Ratio 68
Table 26: Comparison with BAYSIAN METHOD and NTTUA METHOD – Throughput 68
Table 27: Experimental Set Up Baysian 70
Table 28: Experimental Set Up NTTUA 77
Table 29: Experimental Set Up NTTUA 83
Table 30: Percentage Improvement for 100 iterations with 100 nodes 90

Chapter 1: Overview of Wireless Sensor Network

The awesome dynamic research in the area of Wireless Sensor Network (WSN) or Data Sense Point Network (DSPN) has gained lot of attraction among the technical community and research. The job of WSN is to sense the data using detection points, transmit the data to the destination detection point which is connected to a processing center and can be used in multiple span of applications. Wireless Sensor Network (WSN) has the set of data sense points (DSPs). By making use of Detection Placement Strategy (DPS) all the DSPs are spread in an area with each detection point having its own unique location. Delay sensitive applications also have a challenge of forming the complete path at a lower delay constraint. Extending the lifetime ratio is very critical for the use of WSN in applications where removing or connecting the detection point to the energy source is not cost effective and impractical. The other important factor which is responsible for picking the forward node during the route establishment by making use of trust level which will help us to pick the DSPs based on certain requirements in which DSP will respond properly and is sure of taking the data packet forward to the destination DSP. However direct trust sometimes possesses a problem as it considers only the packet delivery ratio for trust computation. Hence more trust parameters must be included in order to improve the forward node pick like finding whether the node is efficient in terms of residual energy, has sufficient capacity to deliver the packet, network loss computation.

1.1 Data sense points

The data sense points (DSPs) can be treated as a location which acquires the useful data and has sufficient capability providing enhancers namely battery along with the sensing device [1]- [6]. Each of data sense points have their own unique identifiers called as sense ids

1.2 Data Sense Area

The data sense area can have all the DSPs placed in a single area or multiple areas. Each area can have a set of DSPs and will have a unique identifier. In Multiple area-based system the DSPs will have unique identifier along with area identifier as well.

1.2.1 Single Deployment Area

This kind of network will have the demarcation created for all the DSPs to be in a single area [6]. Each DSP can communicate to other DSP using its own protocol or algorithm and there is no controlling agent for the path establishment in the network.

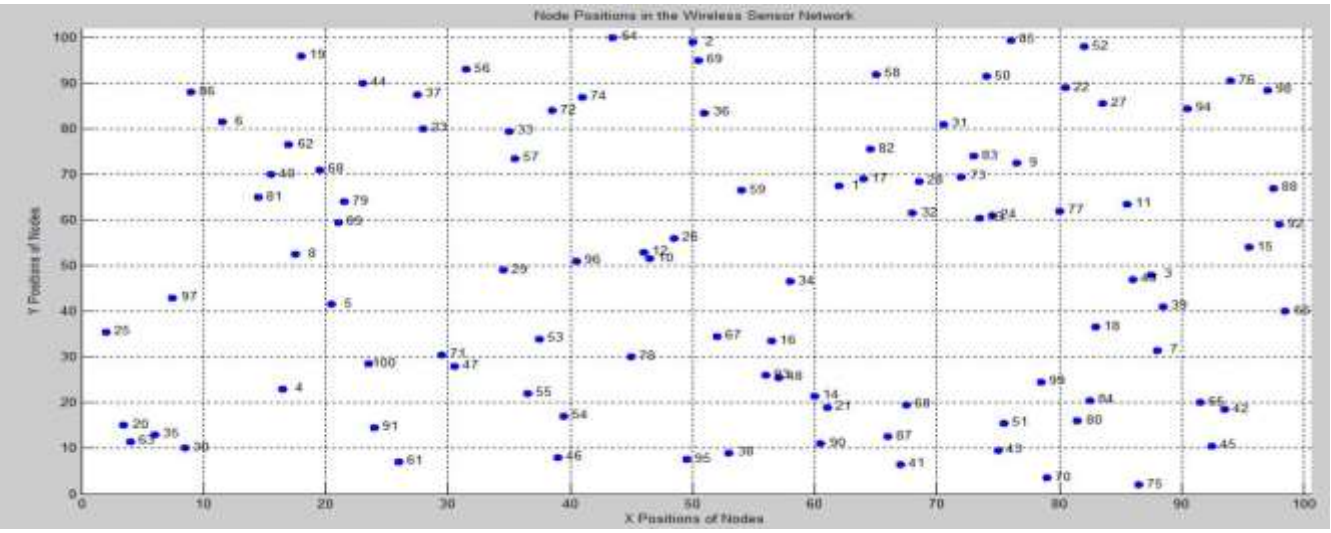

Fig 1: Single Area Sensing Field

Fig1 shows the single area sensing field. As shown in the fig all the DSPs have been deployed within a demarcation boundary of 100*100. Each DSP has its own unique location. For instance, consider DSP 30 which is placed at the location (9,10), In a similar fashion DSP 31 is placed at the location (70,80).

1.2.2 Multi Area Network

For Multi Area based deployment all the DSPs [7] will be placed across multiple independent areas. For the DSP present in a specific area the communication can happen directly with another DSP within the same area. If the DSP for which data must be send is present in a different area, then communication happens through Lead DSP. The Lead DSP is one among the DSPs present in the area selected based on one of the criteria's described in the literature either it can be random or it can be based on remaining energy level or it can be based on distance with respect to receiving DSP or it can be based on combination of energy level and the distance.

The Multi Area Network can be future classified into - Homogenous Sensing Field and Non-Homogenous Sensing Field.

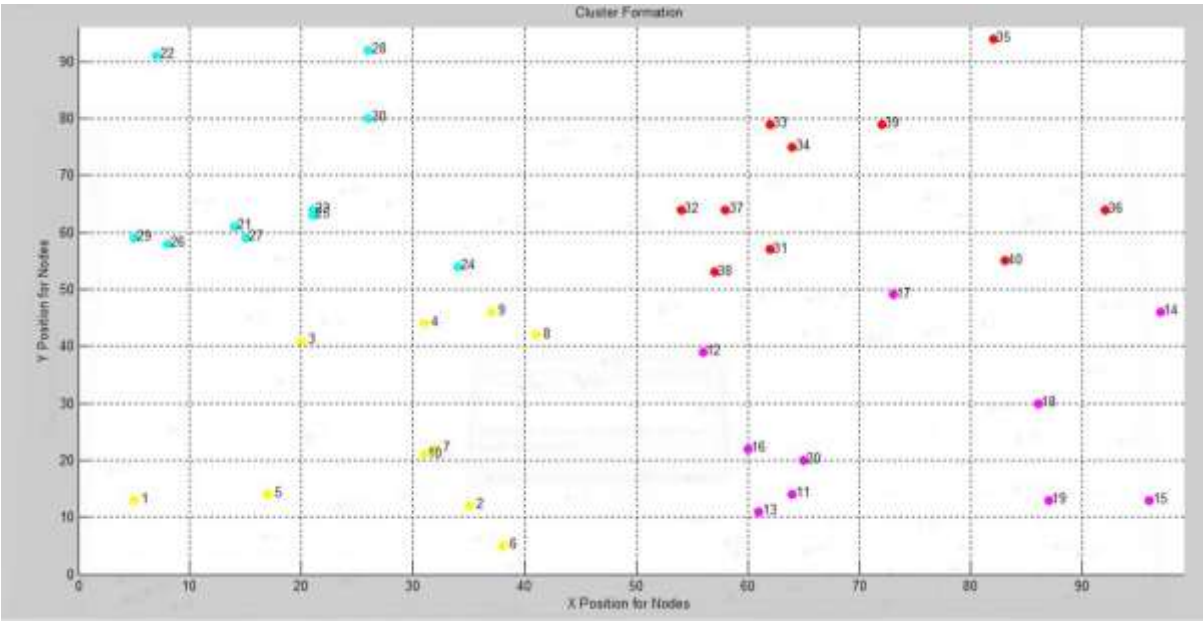

Fig 2: Homogenous Sensing Field

Fig 2 depicts the homogenous sensing field. The entire set of 40 DSPs are present across four areas. Area1 has 10 DSPs namely DSP1 to DSP10. Area 2 also has 10 DSPs from DSP11 to DSP20, Area 3 has the DSPs from DSP21 to DSP30 and then Area 4 has the DSPs from DSP31 to DSP40. Hence a network is called as Homogenous Sensing Field if all the areas have equal number of sensing points.

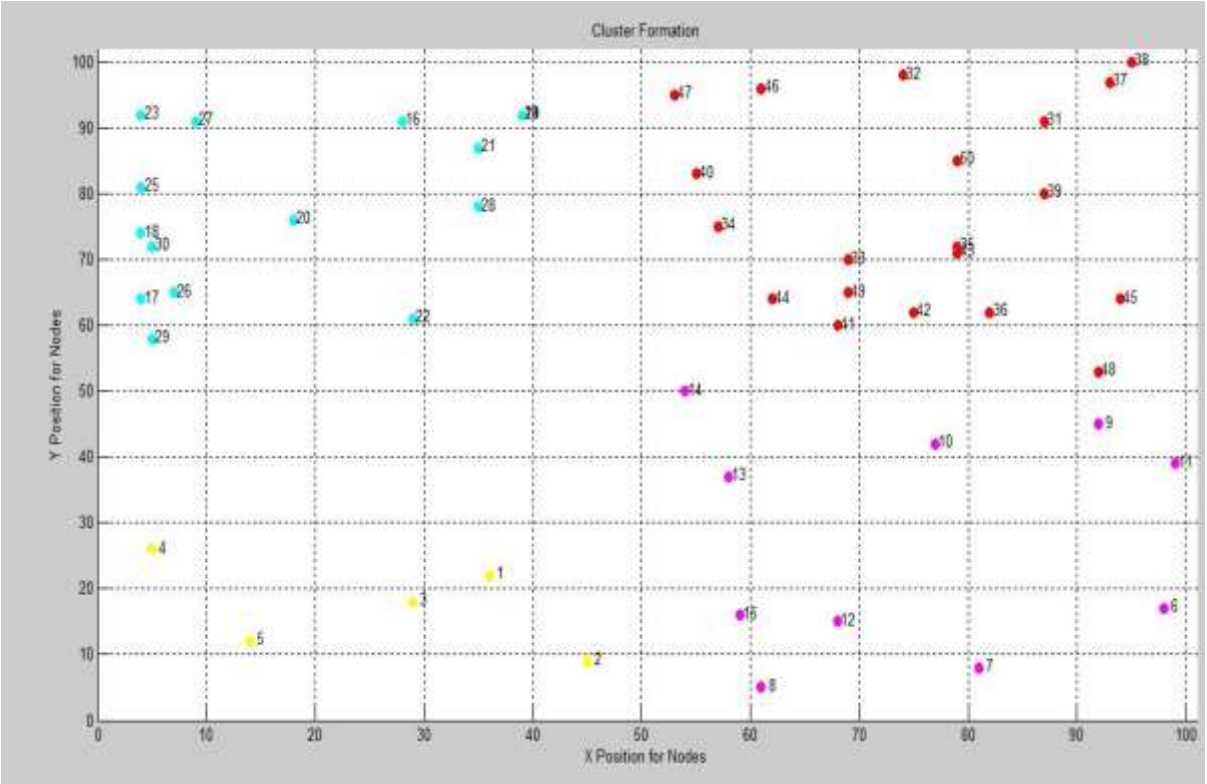

Fig 3: Non-Homogenous Network

Fig 3 shows the Non-Homogenous Sensing Field. As shown in the fig 3 there are different number of DSPs placed under different areas. For Instance, the Area1 has 5 DSPs from DSP1 to DSP5, Area2 has 10 DSPs from DSP6 to DSP15, Area 3 has 10 DSPs from DSP16 to 30 and finally Area 4 has 30 DSPs from DSP31 to DSP60.

1.3 Previous Approach

In the previous approach a trust is computed directly from the initiator DSP to the DSPs which are within the transmission range data sense points regions security the forwarding data sense points is selected based on the behavior of neighbor data sense points the direct trust computation is performed. The previous approach maintains a database at each data sense points level in order to preserve the trust. The base station will send the packets to all the data sense points in the Sensing Field over a period of time and then after that will wait for REPLY.

The ratio of NREPLY/NTRANSMITTED is taken in order to select the next forwarding data sense points in the Sensing Field. The routing mechanism can perform back and forth propagation because of which there is huge amount of energy loss and also since the data sense points delivers the packet the direct trust will also get incremented which is incorrect.

Disadvantages of Previous Approach

[1] The trust computation depends on the Expected Transmission Count which is the direct trust for the DSPs.
[2] There is a lot of energy wastage due to reverse propagation between the DSPs.

1.4 Organization of the Work

The remaining part of the work contains the discussion about the background of various work done for improving the lifetime and security of the network. After that the software requirement analysis is performed for the entire work, the next phase is energy consumption analysis and residual energy computation. The next phase is trust methods which are previous methods and proposed method. The implementation ramifications used to achieve the results are discussed followed by test cases. The results of execution of existing method and the proposal is shown. Also, a comparison is established between the existing method and proposed method. Finally, the conclusion and future scope is performed.

1.5 Summary of the Work

This chapter describes the definition of Data Sensing Point (DSP), DSP networks high level categories along with previous approach

Chapter 2 Methodology

2.1 Research Goals and Objectives

In the proposed method the forwarding data sense points before being selected undergoes a lot of test/parameters measure which is responsible for the picking the forwarding data sense points. It takes into consideration both direct trusts as well as indirect trust in the trust computation. During the trust computation packet loss, energy consumption and packet error rate is taken which improves the accuracy. The routing process in the proposed method maintains a field known as Data sense points in Route which maintains the information of all the traversed data sense points during the routing process. The trust computation is done by taking into consideration the capacity of communication by the DSP along with maintenance of security by the DSP.

2.2 Project Flow

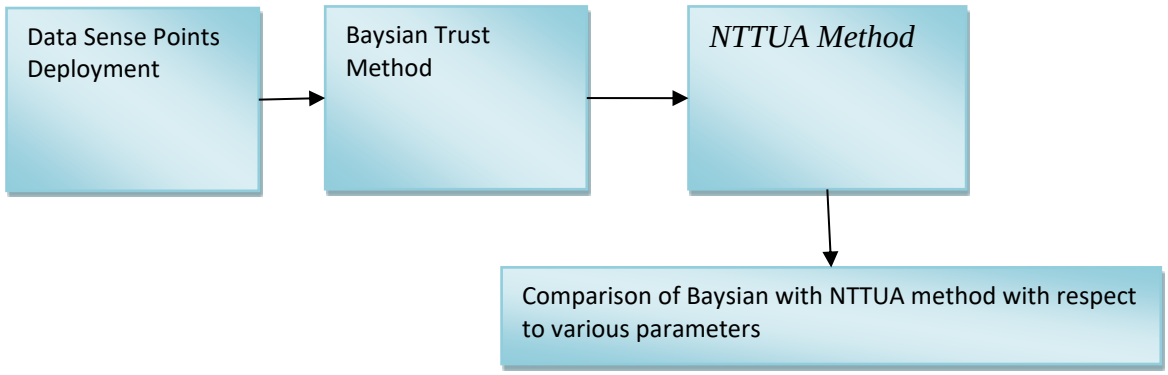

Fig 4: Project Flow

Data Sense Points Deployment

Data sense points Deployment Algorithm is the process which can generate unique location for each DSP along with a unique identifier for each DSP.

Bayesian Trust Method

Bayesian method algorithm finds the neighbors after that pick the DSPs based on the direct trust and then repeat process until destination is reached.

NTTUA Trust Method

NTTUA methods algorithm finds the DSPs within the transmission region after that picks one of the DSP based on direct trust, Sensing Field capability, Sensing Field security and profit loss.

2.3 Comparison Parameters

Time Taken Measure

The time taken for the control packet to traverse from the Source DSP to the Destination DSP and then come back. The time taken can be measured as follows

$$T_{delay} = t_{ack} - t_{send}$$

Where,

t_{ack} = *This is the time at which ACK is obtained from the source DSP*

t_{send} = *This is the time at which REQUEST packet is send from source DSP*

Link Count

Link count is the measure of number of links between source DSP to Destination DSP

Total Energy for Entire Path of DSPs

When the path is formed it will comprise of multiple DSPs between the starting point till the ending point

$$TEDSPPath_c = \sum_{k=1}^{Ndsp} LinkEnergyConsumptionDSP(k)$$

Where,

$Ndsp$ = *number of DSPs link*

$LinkEnergyConsumptionDSP(k)$ = *link energy wasted by the* i^{th} *DSP link*

The Link energy wastage can be computed by using the below equation

$$LinkEnergyConsumptionDSP = 2\,Edsptxn + Edspgen\ disDSPs^{attFact}$$

$Edsptxn = amount\ of\ consumed\ energy\ based\ on\ DSP\ usage\ for\ transmission$

$Edspgen = amount\ of\ consumed\ energy\ based\ on\ DSP\ for\ control\ packet$

$disDSPs = distance\ between\ two\ DSPs$

$attFact = factor\ which\ changes\ based\ on\ temparature$

$0.1 \le attFact \le 1$

Total Overhead

This can be defined as the ratio between the control packet count to data packet count. The method is said to perform well if the value of the total overhead is low.

Total Throughout

It is defined as the number of successful packets delivered to destination DSP in a given complete unit time

It is important to transfer the data between two sensing points (SPs) in a secure manner. The selection of the SPs along the path between initiator sensing point (ISP) and the destination sensing point (DSP) is very important as the SPs along the path are responsible for maintaining the security of the data which is being send. The selection of SPs depends upon various factors and the factor which is considered can be a direct feedback based on the packet transmission rate which internally determines security or based on average transmission rate of packets. One such method is Bayesian trust.

2.4 Research Questions

→ How does existing Bayesian Trust work?

1. The Initiator Data Sense Point (IDSP) and Destination Data Sense Point (DDSP) along with the transmission distance will act as input
2. The DSPs which are within coverage range are found out
3. If the DSPs have the DDSP, then the process is stopped. Otherwise step 4 is executed
4. The next DSP for the path is chosen based on the following steps

a. Send the test packets between IDSP to DSPs within transmission distance in the network.
b. Wait for ACK from DSPs.
c. Compute the ratio of packet send to the ACK received.
d. Repeat the process for the set of N iterations.
e. Compute the aggregated ratio for all DSPs within transmission distance.
f. Pick the next DSP which corresponds to highest value of aggregated ratio

5. Repeat the process from step2 till 4 until DSP is reached.

→What are the drawbacks of Current Method which we are trying to overcome in the proposal?

1. The process of selecting the DSPs depends on the aggregated ratio process which is time consuming.
2. During the selection of DSPs since there is no trace maintained along the path there is high probability of back and forth propagation which leads to more number of hops
3. The energy consumption for the path can be computed as the aggregation of all the link energy across the path. The energy consumed for each specific link is computed using the below formula

$$LinkEnergyConsumptionDSP = 2\,Edsptxn + Edspgen\ disDSPs^{attFact}$$
$$Edsptxn = amount\ of\ consumed\ energy\ based\ on\ DSP\ usage\ for\ transmission$$
$$Edspgen = amount\ of\ consumed\ energy\ based\ on\ DSP\ for\ control\ packet$$
$$disDSPs = dis\tan ce\ between\ two\ DSPs$$
$$attFact = factor\ which\ changes\ based\ on\ temparature$$
$$0.1 \le attFact \le 1$$

As stated in point 2 as the number of links increases the consumed energy increases due to dependency on distance

4. The repeated participation of the DSPs in the routing path will lead to more energy consumption of the specific DSPs which eventually will lead more number of in-efficient SPs in the network and will affect the lifetime

→ The Research Proposal how does it overcome the drawbacks

1. The research proposal will make use of trace list which prevents back and forth propagation between DSPs as the entire DSP list is appended to the control packet
2. The selection criteria for DSP will be improved by making use of multiple factors for the DSPs within the transmission distance those include compute network security, profit loss and network capability.
3. Eventually when the existing method is compared with the research proposal with respect to delay, energy consumption, in-efficient nodes the proposal will perform in a better fashion.

Bayesian based system model makes use of multi point system which computes the different aspect of trusts based on behavior of DSPs but the disadvantage of this approach is that it makes use of only a direct computation of trust [32]. Hence the proposal will make use of more criteria to compute the trust including residual energy, direct trust, network capability and network profit.

2.5 Sensing point Placement Strategy

The Sensing point placement method is responsible for generating the location of the DSPs and then providing them a unique identifier. The number of DSPs which are to be placed in the given area and the area end points will act as an input. First the unique identifier for the DSP will start with a value of 1, the x and y position for the DSPs are chosen randomly between the end points of the area and finally a tuple is formed with {unique identifier integer, position of DSP}

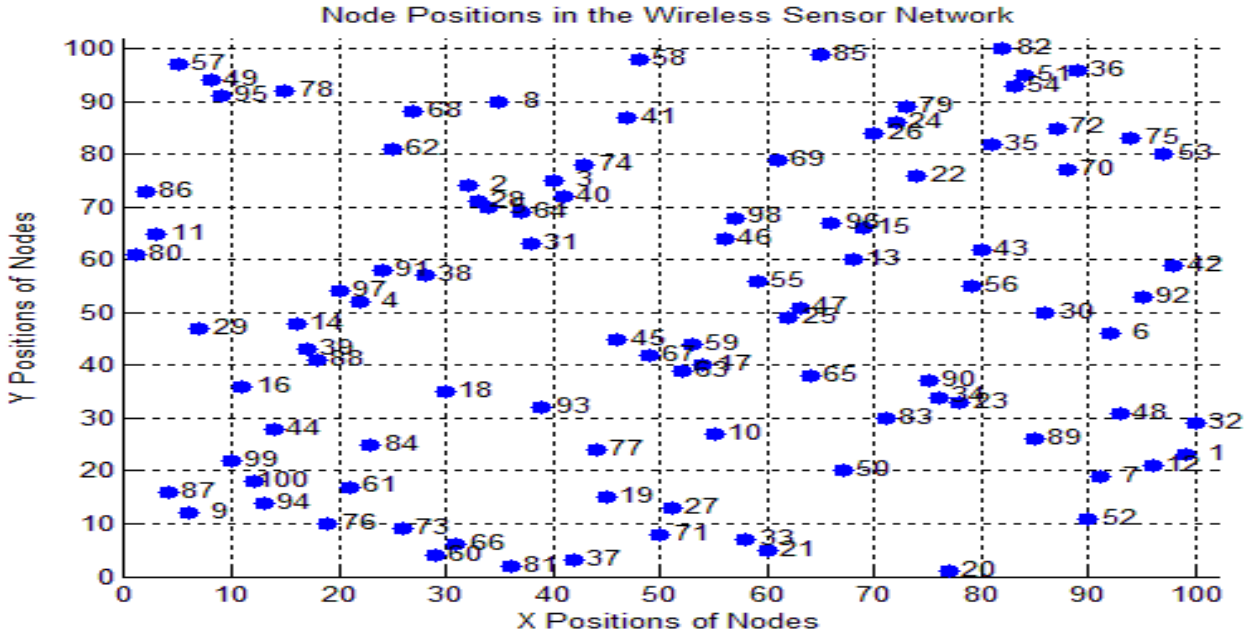

Fig 5 Initial Location for DSPs

Fig5 shows the 100 DSPs placed in a boundary limit of 100*100 meters. Each of the DSPs have their own unique location in the area. There are multiple caveats which limit the DSPs network like energy restrictions, range restrictions, memory capability along with link bandwidth. Path establishment is one of the most significant factors which needs to work even under worse energy restrictions and more value provided to residual battery power during the DSP picks in the path establishment. At different time intervals the DSPs will be located at unique locations as depicted in the network model of Fig 6

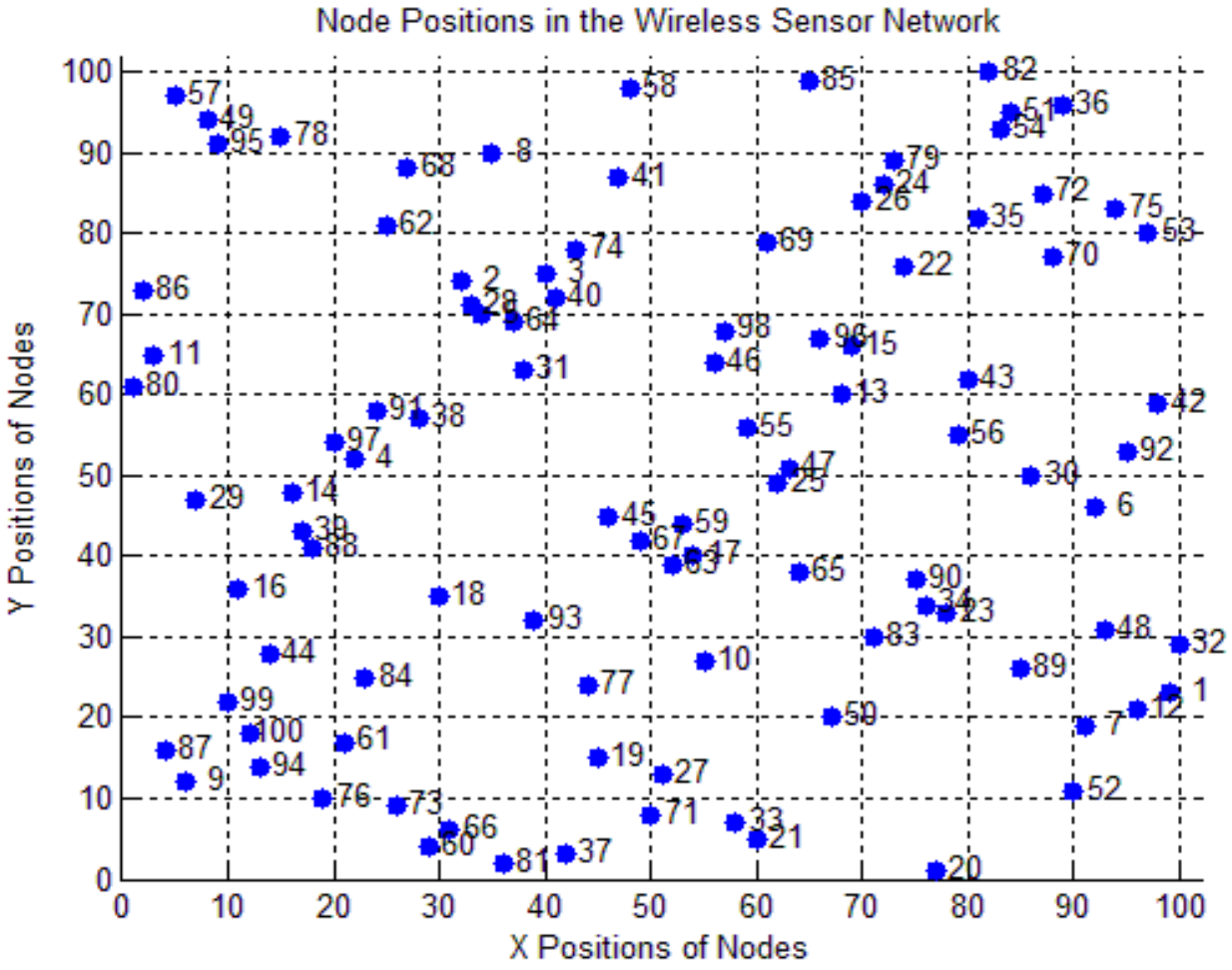

Fig6 *DSPs* Location for Iteration1

The Fig 6 depicts that the DSPs have their own locations and all the DSPs do not cross the area limits of 100*100. Also, no two DSPs have their location which is colliding in nature.

DSP 32 is at the location (100,29), DSP 100 is at the location (12,18). In a similar fashion each of the DSPs are at their own unique location. Also, one can note that the location of DSP 32 is not colliding with location of DSP 100. No two DSPs have the same locations and hence satisfy the boundary conditions of area limits.

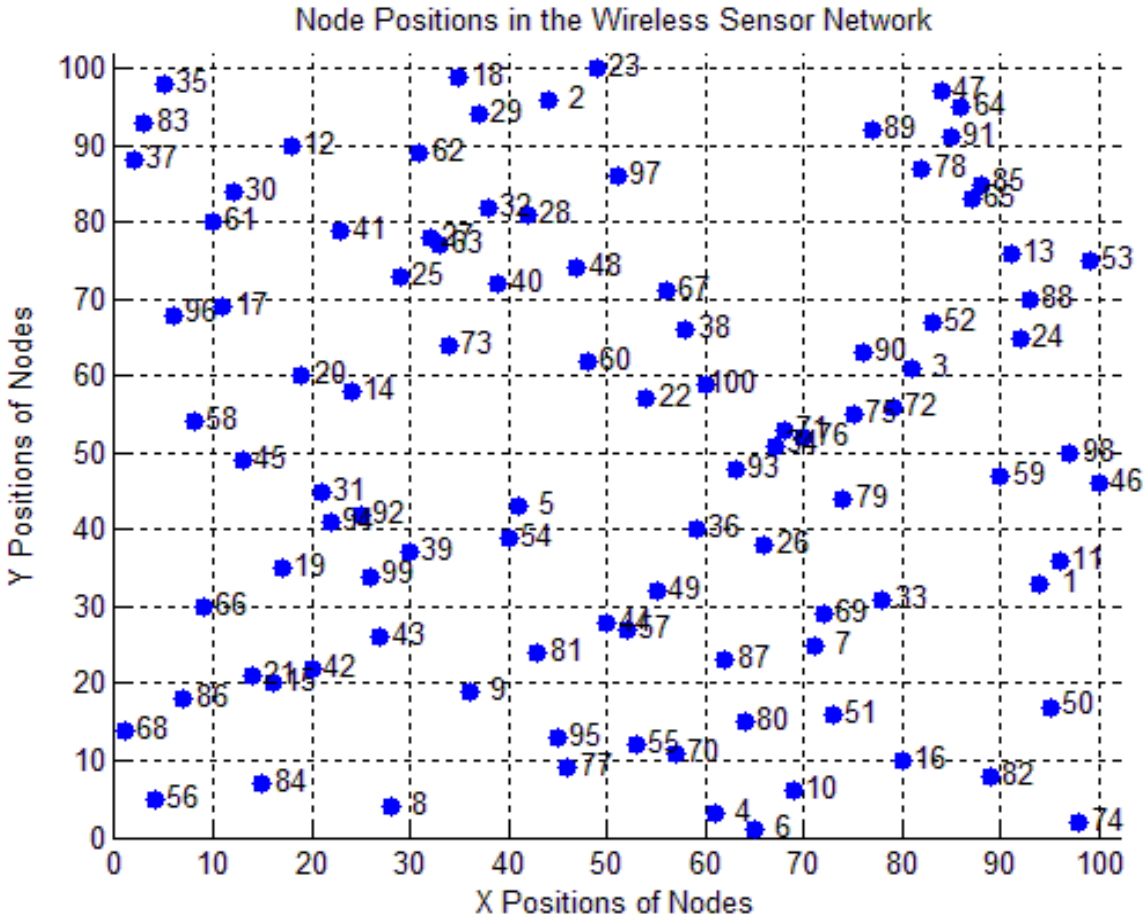

Fig7 DSP Locations for Iteration=2

Fig 7 shows the location of DSPs this time after certain time T. As shown in the Fig 7 each DSPs have their own unique location. DSP 32 is now at a different location which is (40,81) which is different from the location used for iteration1 and DSP 100 is at a different location which is (60,59).

The same is summarized in the following table

DSP Identifier	Location during Iteration1	Location during Iteration2
32	(100,29)	(40,81)
100	(12,18)	(60,59)

Table1 Location for DSPs

After the execution of the two iterations. From Table1 one can observer that the DSPs have changed their positions in the network. This can be future extended for multiple iterations over the network. After 5 iterations are executed and for each iteration the DSP is represented with a different color as depicted in the Fig 8

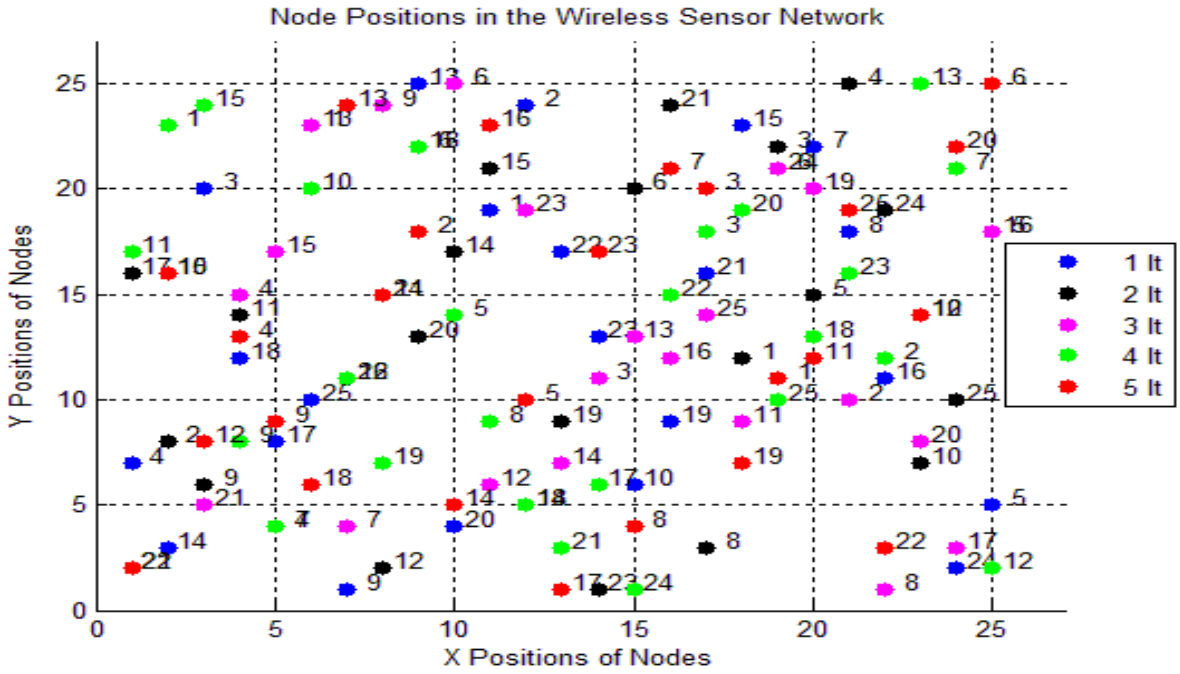

Fig8 Location Changes for all DSPs

Fig shows the result of the experiment which is repeated five times and then change in position for the DSPs is observed for each iteration. Also, the position of the DSPs is represented with a unique color for each iteration. For the experiment the number of DSPs considered are 25. Across all iterations the DSPs maintain the boundary conditions and change their positions.

2.6 Mathematical Modeling for DSPs Placement

Consider a space with the end points namely $Px_{\min}, Px_{\max}, Py_{\min}$ *and* $Py_{\max}$. The DSPs represented by a 3 parameter $(B, M.A)$ Battery, Memory and Antenna are set of entities which must satisfy the conditional end points $Px_{\min} \geq Px_k \leq Px_{\max}$ and $Py_{\min} \geq Py_k \leq Py_{\max}$. Px_k, Py_k represents position of the k^{th} DSP in the area. Since one DSP cannot take the same physical location as that of other DSP in the area. The network model of Detection Sensor Network (DSN) must satisfy the condition $(Px_n, Py_n) \neq (Px_m, Py_m)$. Px_n, Py_n Represents the position of n^{th} DSP and Px_m, Py_m represents the position of m^{th} DSP in the area. For the network model there will be many DSPs N_{nodes} which will aid in the routing process across various layers of protocol stack. Finally, each of the DSPs must be described using the 3 unique attributes namely DSP unique identifier and respective location of DSP in the network. If there are N_{nodes} then a matrix must be created as

DSP Identifier	Location
DSP1	(Px_1, Py_1)
DSP2	(Px_2, Py_2)
DSPN	(Px_n, Py_n)

Table 2: DSP Locations

Table2 is a generalized matrix which depicts the various DSPs and their respective locations in the network. The location of various DSPs is unique in nature.

The mathematical formulation for DSP placement for Simulation can be described as below

Algorithm1: Data Sense Point Placement

Input: $N_{nodes}, x_{\min}, x_{\max}, y_{\min}, y_{\max}$

Output: DSP Locations and Unique Identifier NI

Description:

a) $z = 1$

b) $z : 1 ---> N_{dsps}$

c) Generate the position of DSP in the random fashion which follows the protocol

$Px_z = v$ *any* v *which satifies*

$Px_{\min} \le Pv \le Px_{\max}$ & $Pxv \neq Px_h$

$Py_z = v$ *any* v *which satifies*

$Py_{\min} \le Pv \le Py_{\max}$

and $v \neq y_H$

Px_H – *history of x positions previously assigned*

&

Py_H – *history of y positions previously assigned*

e) The unique identifier along with position are formed as below (*uniqueIdentifier, position*))

f) Store in the z^{th} row of Matrix

Unique Identifier	Position of DSP
z	(Px_z, Py_{iz})

g) z=z+1 Note – Internally each value of zhas a unique address for communication

Fig 9 Mathematical Model for DSP Placement

2.7 Energy Utilization Process

The energy utilization in a DSP network is based on the radio propagation models which are present in the papers [1]-[4]. Consider that there are two detection points DSP 1 and DSP 2 and distance between the detection points is ‘dis’. The amount of transmission bits

by the DSP is Namount. Each DSP will have an amplifier circuit along with transmission device as shown in the Fig10

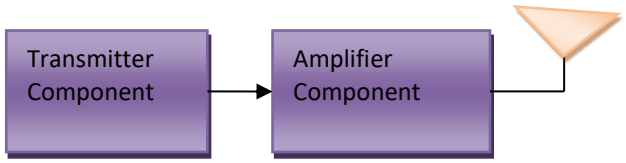

Fig10 Energy Consumption Model

The energy utilization for transmission over a link can be defined using the equation (1)

$$E_{consumedtrans}(N_b, d) = N_b * (E_{transmittercircuit} + E_{reception} * d^n) \quad (1)$$

Where,

$N_b = Number\ of\ bits$

$d = distance\ value\ between\ DSPs$

$E_{transmittercircuit} = energy\ required\ by\ transmission circuit$

$E_{reception} = energy\ required\ by\ reception$

$n = a\ constant\ integer$

The energy utilization during the reception of the data is defined using the equation (2)

$$E_{consumedreception} = N_b * E_{tranmitterciruit} \quad (2)$$

The total energy utilization for both transmission and reception is given by

$$E_{consumedtotal} = E_{consumedtrans} + E_{consumedreception} \quad (3)$$

Substituting the values present in the equation 2 and equation 1 in equation 3

$$E_{consumedtotal} = N_b * (E_{transmittercircuit} + E_{reception} * d^n) + N_b * E_{tranmitterciruit} \quad (4)$$

Multiplying the expression Nb outside the bracket with the contents of the bracket

$$E_{consumedtotal} = N_b * E_{transmittercircuit} + N_b * E_{reception} * d^n + N_b * E_{tranmitterciruit} \quad (5)$$

Now performing the addition of the similar items in equation (5) will result in

$$E_{consumedtotal} = 2 * N_b * E_{transmittercircuit} + N_b * E_{reception} * d^n \quad (6)$$

Taking the value of Nb Out of the two expressions from equation (6)

$$E_{consumedtotal} = (2 * E_{transmittercircuit} + E_{reception} * d^{n}) * N_{b} \quad (7)$$

The entire energy utilization modelling is performed based on the radio propagation models given in the literature. The sensing point has majorly main components like transmitter component and amplifier component

$$E_{c} = 2 * N_{b} E_{transmitter} + N_{b} * E_{reciever} * d^{n}$$
$$E_{c} = N_{b}(2 * E_{transmitted} + E_{reciver} * d^{n})$$

From the Classical Energy Consumption, the energy required for transmission and receiver energy are provided in table 3

Mode of Operation of Antenna	Energy Consumption
$E_{transmitter}$	50 nJ/bit
$E_{reciever}$	100 pJ bit/m

Table 3: Classical Energy utilization values

There is a direct dependency between energy and distance. As per the computation the energy utilization increases as the distance between the detection points increases. In a similar fashion energy is also consumed for sensing point m when it transmits data to destination z.

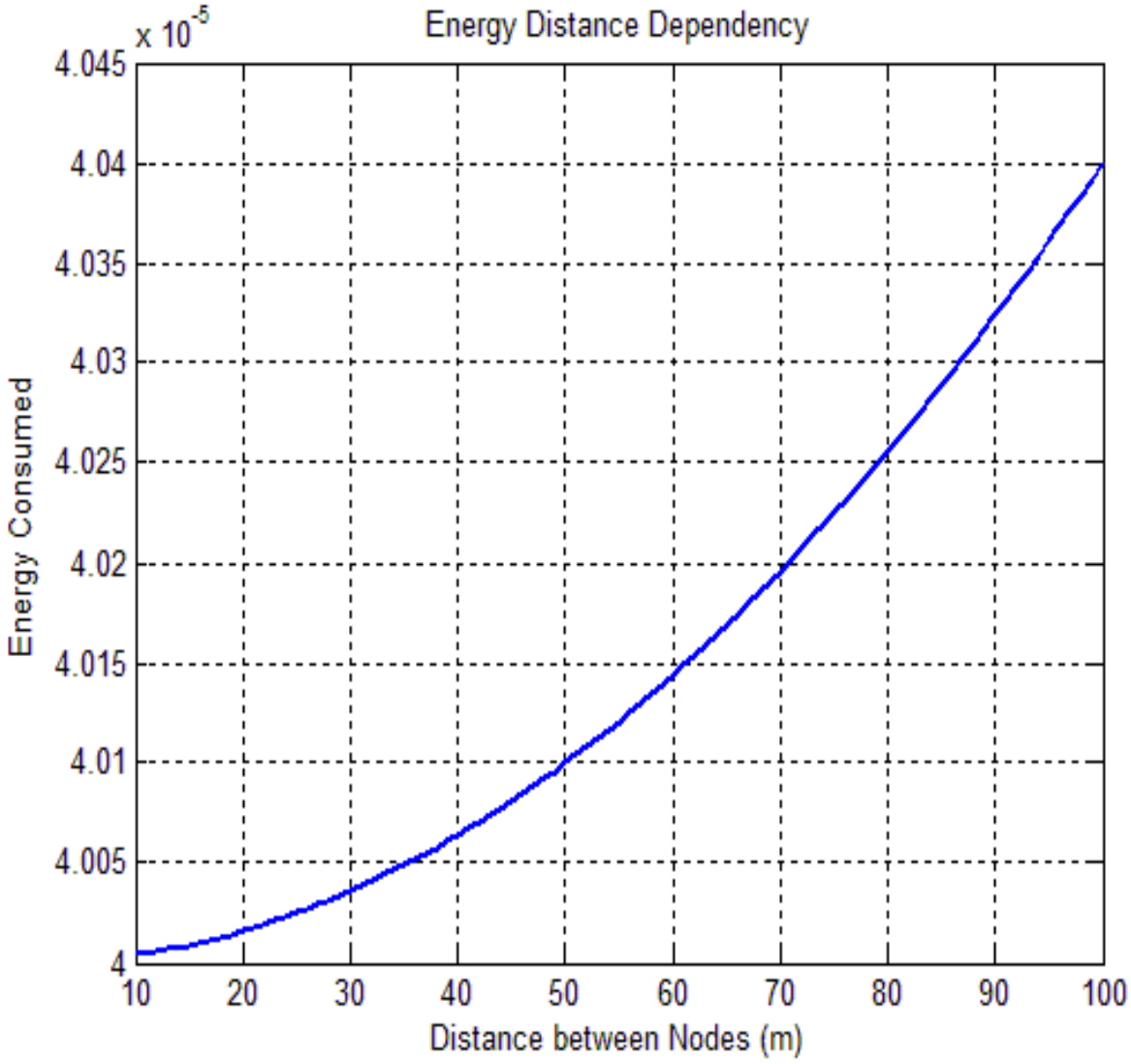

Fig11 Energy Consumption Distance

During the Network initialization phase all detection points will have the same amount of initial energy. When the sensing point participates in the path finding then the participating sensing point will reduce the amount of energy levels by making use of $UE_f = CE_f - E_c$. The threshold is IB/4 where IB is the initial battery during network initialization. Fig 11 indicates the distance variation from 10m to 100m versus the energy consumed.

2.8 Distance communication Set

Consider that the set of DSPs which are arranged in a linear fashion and each DSP is separated by other sensing point with the distance of 20 m between them.

1→2 →5→4→5→6→7→8→9→10

For DSP1 the distance with respect to other DSPs in the network are defined as below

DSP Unique Identifier	Distance
1	0
2	20
5	40
4	60
5	80
6	100
7	120
8	130
9	140
10	160

Table4 DSP1 distance with respect to other DSPs

The table4 shows that the distance between DSP1 to other DSPs in the network. The distance between DSP1 to itself is zero, the distance between DSP1 to DSP2 is 20m in a similar fashion the distances with respect to various DSPs are computed.

The distance communication sensing point set details flowchart are given below

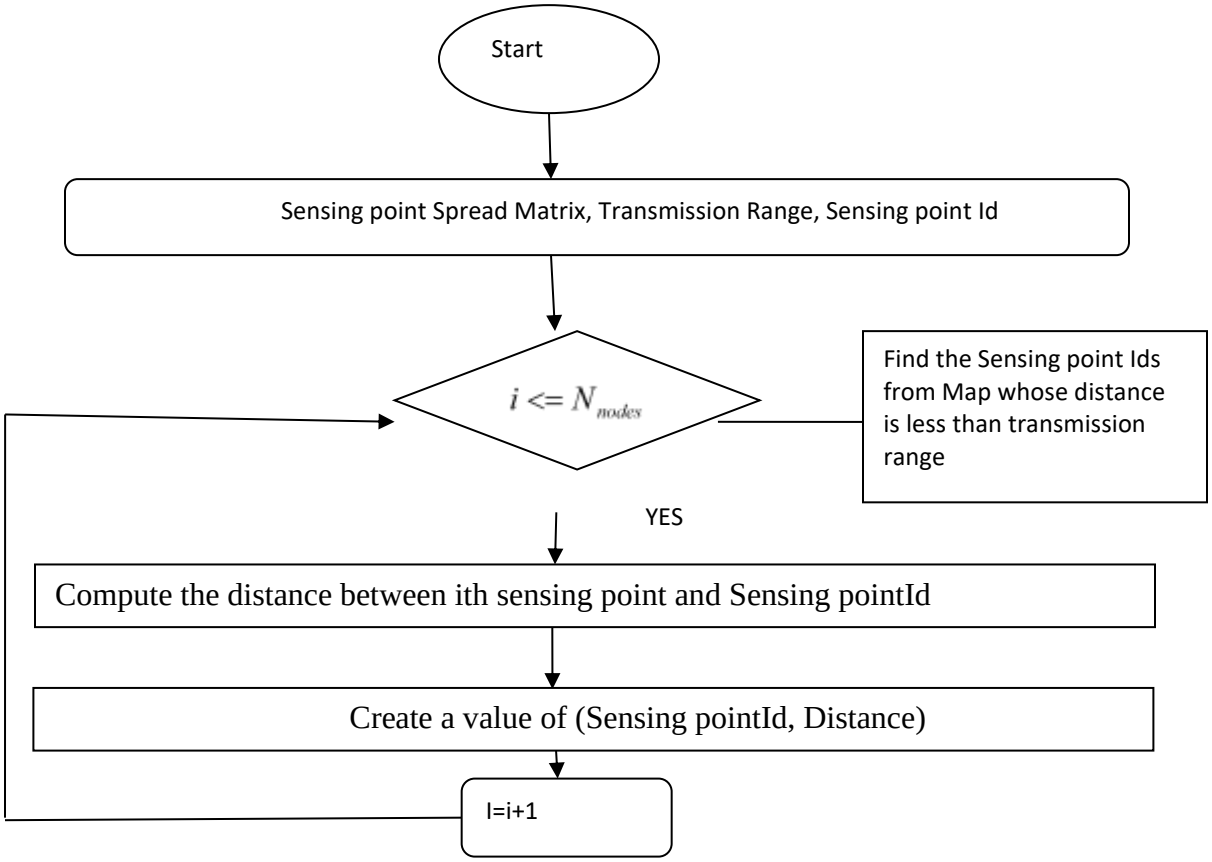

Fig12 Distance computation between DSPs

The following are the steps which are present in the Distance computation between DSPs

1. DSP Spread Matrix, Transmission Range and DSP Id
2. Find the count of number of DSPs in the Sensing point Spread Matrix
3. Start from the 1st DSP till the Number of DSPs Compute the following
    a) Compute the distance between ith DSP and Sensing point ID
    b) Put the DSP Id and Distance within the Map
    c) Increment the value of i
4. Finding the DSP Ids in the map whose distance is less than transmission range

2.9 Classification of Efficient and Non-Efficient Set Analysis

If IBE is representing the initial battery energy during network initialization, then the DSPs can be classified as Non-Efficient and Efficient DSPs.

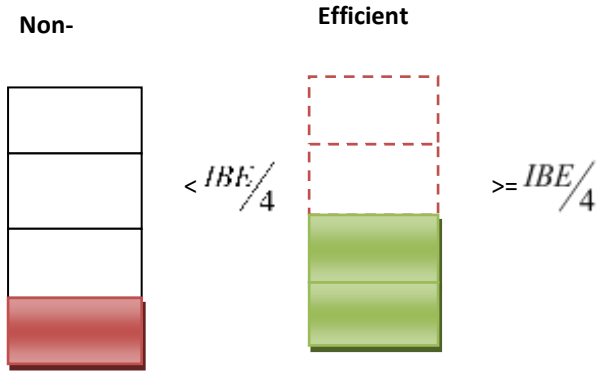

Fig 13: Efficient and Non-Efficient DSPs criteria

Fig 13 shows the different kind of DSPs which are present in the network. In an area of 100* 100 m there are 10 DSPs which are placed, and all the DSPs have the initial battery value with a value of 500 J.

DSP ID	Battery Energy
DSP1	2000
DSP2	2000
DSP3	2000
DSP4	2000
DSP5	2000
DSP6	2000
DSP7	2000
DSP8	2000
DSP9	2000
DSP10	2000

Table 5 Initial Battery Energy

Table 5 depicts that all the DSPs from DSP1 to DSP10 are having the same value of battery energy even before the path establishment is initiated. All DSPs have 500 J of first level of energy.

The threshold value for classification is IBE/4 which becomes 125 J. Consider that the path between the IDSP4 to DDSP10 is as follows DSP4→ DSP7→DSP8→DSP10. The distance between the DSPs can be assumed to be as defined in the table 5

Link between DSPs	Distance of the Link
DSP4→ DSP7	20.24
DSP7→DSP8	45.56
DSP8→DSP10	54.56

Table6 Distance between Detection points

The DSPs which are in the path will lose their energy levels based on transmission energy, generation energy, distance and other environment factors.

The energy updates for the DSPs are computed by using the following formula

UE(DSP)= CE(DSP) – Ec(Link)

Where,

CE(DSP) = current energy of DSP

UE(DSP) = update energy of DSP

Ec(Link)= Energy consumed between the DSPs

Considering the values for the various parameters for DSPs energy utilization as described in Table 7

Parameter Name	**Parameter Value**
Energy required for Transmission by DSP	20 J
Energy required for Generation by DSP	10 J
Attenuation Factor	0.5

Table7 Energy Utilization Value for DSP link

The updated energy of DSP4 to DSP7 can be computed as below

UE4= CE4- Ec(47) = 500- (2* 20+ 10* d47^0.5) = 500– (2*20+10*20.24^0.5) = 415.0111 J

In a similar fashion the updating of DSP 7 energy level and DSP 8 energy level

UE7= CE7- Ec78 = 500- (2* 20+ 10* d78^0.5) = 500 – (2*20+10*45.56^0.5) =392.5019 J

UE8= CE8- Ec810 = 500- (2* 20+ 10* d810^0.5) = 500 – (2*20+10*54.56^0.5) = 386.1353 J

The updating of energy levels after the routing path is established is given by

DSP ID	Residual Energy
DSP1	500
DSP2	500
DSP3	500
DSP4	415.0111 J
DSP5	500
DSP6	500
DSP7	392.5019 J
DSP8	386.1353 J
DSP9	500
DSP10	500

5.

Table 8 Residual Energy after iteration 1 of path establishment for DSPs

Table 8 shows that the DSP4, DSP7 and DSP8 have their energy levels reduced as they have been used in the path. When the DSPs are used for multiple paths establishment over a period of time the battery levels of such DSPs will come down.

Consider after a period of 100 iterations the following is the energy level of the detection points in the network.

Sensing point ID	Residual Energy
1	105.45
2	400
5	389
4	324.67
5	500
6	250.57
7	500
8	500
9	80.87
10	1000

6.

Table 9 Residual Energy after 100 iterations of path establishment

As shown in the Table9 DSP1 and DSP 9 are Inefficient DSPs and remaining DSPs are efficient

2.10 Summary

This chapter describes the research and goal of the project, project flow, the various research questions and how the proposed method overcomes the disadvantages, energy utilization and battery level reduction of energy levels.

CHAPTER 3

LITERATURE SURVEY

This chapter deals with the various work done in the literature related to WSN, Energy consumption analysis, lifetime ratio analysis and trust computation analysis.

3.1 WSN

When multiple subjects like mechanical, wireless, electronics. The data collection [1] will happen from the data sense points (DPs) and then the sensed data is sent towards the receiver data sense points (DPs). The process improvement [2] is done with the help of industry based wireless sensor networks (WSN) in order to improve efficiency and good industry-based productivity. There are various advantages of WSN like auto organization, deployment of data sense points (DPs), generation of data sense points (DPs). The area of multidisciplinary applications will be used between users for making collaboration, to build software applications for society [3]- [6].

DSPs set are used in different kind of applications. The zones are built by the workers [7] and then the task of detection for the data is done with the help of DSPs which have various characteristics like lower monetary compensation, smaller size, ability to reuse by using washing process and then better efficiency. The use of DSPs in this application is the amount of allergy faced by workers due to dust along with exposure to ultraviolet based rays [7].

The amount of muscle strain can be sensed by making use of Electromyogram (EMG) device [8]. There is a need for a solution in which the signal whenever it is generated by EMG device can be sent to network which can forward to a region outside EMG sensor area. The results from the EMG sensor data sense can be sending to physician who is residing far away from patients.

The decrease of carrier frequency to 180 MHz along with narrow band channels provides robust interference [9], non-line of sight (NLOS) coverage and can be applied for cultivation regions so that sustainable agriculture can be maintained.

3.2 Energy Consumption

WSN is used for wide variety of applications like medical transmission, environment data, and transportation [10]. Retransmission mechanisms and redundancy are used to improve reliability. The retransmission and redundancy does not take into consideration energy consumption constraint and hence multipath routing is used for reducing the energy consumption and higher reliable data transmission.

The energy conservation in the network [11] can be achieved by making use of better communication techniques in which data sense points are gathered into a group known as area. The data sense points will send the data to the region head and then the data is delivered to controller level sensing point. In a Centralized Selection approach, the sensing point which is closer to the center of the specific area is chosen as the area head. Whenever a single sensing point consumes more energy than the other sensing point it leads to becoming of dead sensing point. Virtual Grid based Dynamic Routes Adjustment (VGDRA) algorithm has better energy efficiency as compared to leach due to better load balancing and then makes use of less number of loops.

Two important issues namely energy modeling and energy consumption computation helps in the optimization of WSN sensing point [12]. The energy model which takes into consideration both MAC and physical layer is considered and measured for both AWGN and Non-AWGN channel.

The sensor data sense points will be combination of communication capability, data conditioner and sensing capability [13]. The batteries will drain out to energy levels quickly which reduces the energy efficiency. The mean energy level, dropping ratio and latency are

important parameters along with MSK or OQPSK16 can be used to control the amount of energy being used.

The amount of processing capability used to process [14] and to enhance cross layer collaboration in WSN the architecture is divided into multi hop task mapping and multi hop scheduling to reduce the energy consumption in WSN.

The better design for WSN involves the minimization of energy consumption [15] in which energy consumption model is done based on physical layer parameters for Rayleigh fading channels. The minimum energy consumption is done based on optimized transmitted power.

WSN is a collection of data sense points [16] which senses the information and then sends towards the sink. WSN data sense points have limited energy, limited storage and processing power and WSN existence depends on the life of sensor data sense points. The data sense points are grouped into zones and then zone formation depends on the remaining energy of data sense points. The packet flow will be from normal data sense points to cluster heads; after that it will happen from CH to BS.

The algorithm which finds the energy dependency will have two phases [17]. The first phase will be profiling which will allow the network to be run 800 times for different parameters in order to compute the average energy and in the second phase parameter extraction is used compute p-value, non-linear and linear correlated values.

The data reduction [18] based on threshold is used in data pre-processing in order to perform the reduction in the energy-based value. The removal of redundant data is done at sensor sensing point and can be used to collect data

3.3 Lifetime Value Computation

The working of the area containing DSPs can be achieved with the help of better lifetime ratio [19]. The data transmission process reduces the battery levels of the DSPs in the link based on link transmission, link generation and distance between the two DSPs along with factor which depends on temperature or humidity. Consider a symbolic representation LT which is time taken

for the DSPs to have their remaining energy less than threshold value [20]- [23]. The value for lifetime can be defined by various factors as below

Lifetime Value (LV)	**Lifetime Value Details**
LV-1	When the value of LV is within the boundary conditions of SNR based on QOS until the time T [24].
LV-2	When the data can be sensed by at least one DSP for certain time period [25]
LV-3	Amount of time it takes for the head DSP to have its energy level declined to a value of zero [26]
LV-4	Suppose the threshold value of amount of packets to be send to destination DSP is around 27.85% then time it takes to reach below this value of 27.85% is defined as LV [27].

Table10 Definition of Network Lifetime

3.4 Trust Level Computation

The resource allocation is a critical issue in the field of DSPs network. The cost ramification which is responsible for achieving better resource allocation is usually achieved by taking a set of operators. Another challenge is the computation of cost ramification along with its maintenance due to communication-based errors or because of invalid convergence in the equilibrium. Non

smooth based Lyapunov analysis is performed on the public DSPs to check the malicious information being spread in the area [28].

With the technology advancement most of applications are going with IOT device-based technology but the problem with such a network is security. The devices can be hacked using techniques like horizontal based port scans. The software - defined based DSP area along with firewall can be used to reduce the security concerns caused by such scans. FleXight platform used by the authors provide the access to information within the packet so that security layer can be added keeping in mind the overhead ratio [29].

The cloud-based system provides variety of services for various industries. The major concern is the safety of the data and then intrusion happening in the system which is measured by making the computation of trust level values. The techniques used to identify the intrusion can be either label-based machine learning or a cluster-based machine learning. label based methods are very weak to provide the security. Ensemble system with trained data which is generic in nature along with fuzzy method helps in classification of intrusion-based DSPs and picking a DSP which is not compromised [30].

The intrusion happens on the network by using behavior analysis of the DSPs. The security of the DSP network can be improved by making use of IPS tool. An approach which can detect the violation of the security policy along with detection of security is defined [31].

DSP based network are used for critical applications where security is a paramount concern. The DSP based networks have limited resources and hence are subject to security attack. Black hole-based attacks will have effects on the value of data collection. Active Trust is a technique which will avoid the of black holes to form the route which in turn achieve efficiency and security [32].

3.5 Summary

This chapter deals with the various work done in the literature related to WSN, Energy consumption analysis, lifetime ratio analysis and trust computation analysis.

CHAPTER 4
SOFTWARE REQUIREMENTS SPECIFICATION

The focus of this chapter will be on the different software's that are used for the implementation of Bayesian trust method along with NTTU method. This will also indicate what are the ramification requirements and non-ramification requirements along with the hardware and software requirements. MATLAB is a programming language especially designed for research purposes. It has support for numerous ramifications and toolboxes which provides lot of ramificationalities with respect to multiple domains. The various toolboxes available in MATLAB are described in Fig 14

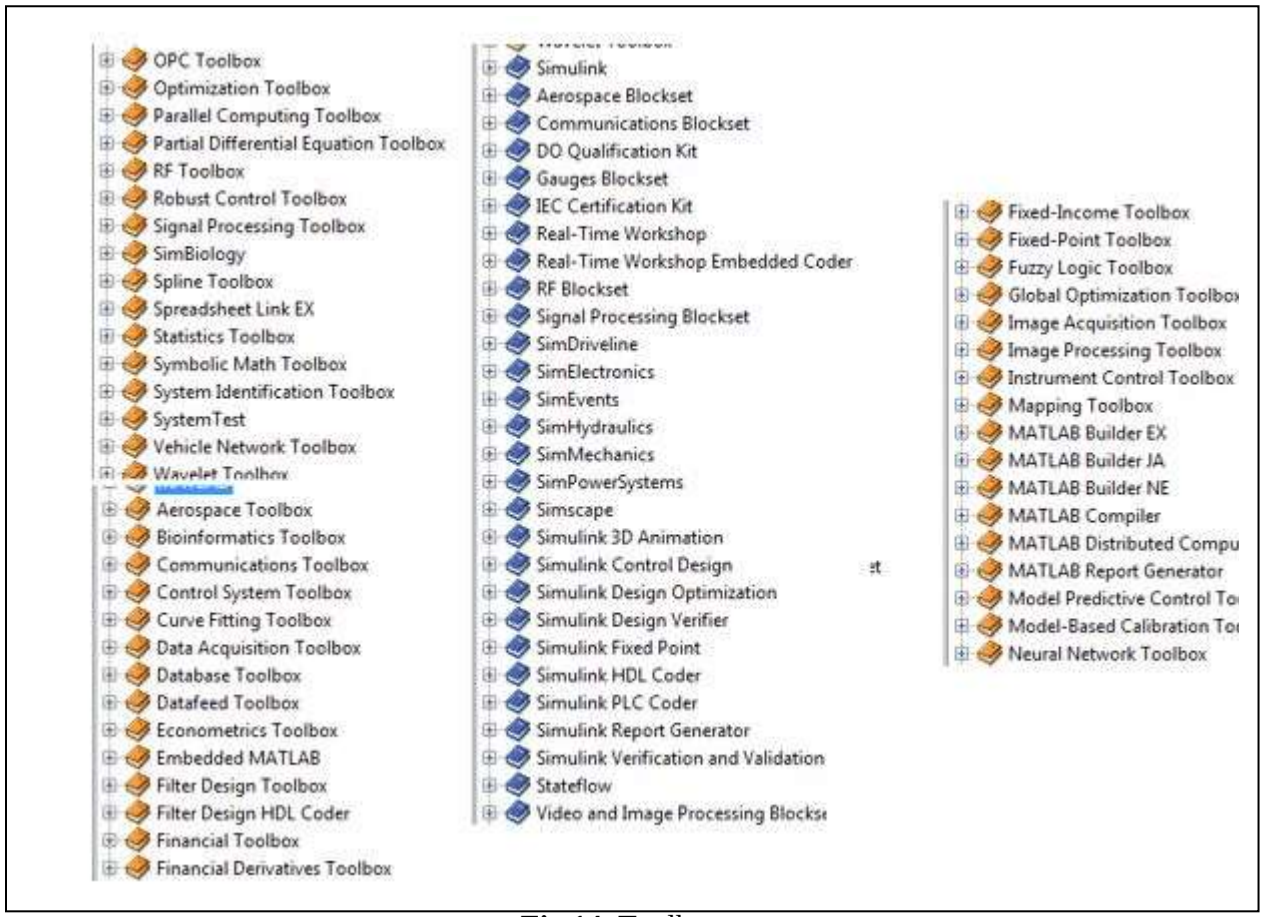

Fig 14: Toolboxes

4.1 Functional Requirements

Requirement Name	**Requirement Description**
Placement of Data Sensing Points	This module should have the capability of placing the DSPs in the network along with generation of unique identifier
Distance Computation	This module should have the capability of computing the distance of each DSP to every other DSP in the network
Transmission Range DSP Detection	This module should have the capability for finding the DSPs within the coverage range
Baysian Trust Method	This module should have the capability for path establishment between the initiator DSP to destination DSP based on direct trust computation The direct trust must be computed by sending the test packets between IDSP to DSPs within transmission distance in the Sensing Field, waiting for ACK from DSPs., Computing the ratio of packet send to the ACK received, Computing the aggregated ratio for all DSPs within transmission distance and then selecting the next DSP which corresponds to highest value of aggregated ratio
NTTU Trust Method	This module should have the capability for path establishment between the initiator DSP to destination DSP based on
Energy Consumption Computation Method	This module should compute the link energy consumed for the given transmission energy, generation energy, distance and attenuation factor
Residual Energy Computation Method	This module should have the capability of updating the battery levels of the DSPs who participate in the route establishment and reducing the energy levels of the DSPs based on current battery level and energy consumed over the link
Comparison Parameters	This module compares between Baysian and NTTUA method and proves that NTTUA method behaves the best

Table 11: Functional Requirements

4.2 SOFTWARE AND HARDWARE REQUIREMENTS

Sl no	Parameter Name	Parameter Value
1	RAM	8GB
2	Hard Disk	320GB
3	Programming Language	MATLAB
4	MATLAB Version	MATLAB 2010

Table 12: Software and Hardware Requirements

4.3 HIGH LEVEL DESIGN

The high-level design will discuss about the data flow diagrams for the project

Data Flow Diagrams

Fig 15: DFD Level 0

Fig 15 shows the DFD Level 0. The inputs for the DFD Level 0 are Number of DSPs, IDSP, DDSP, Initial Battery and Transmission Range. The Output is Path Established from IDSP to DDSP.

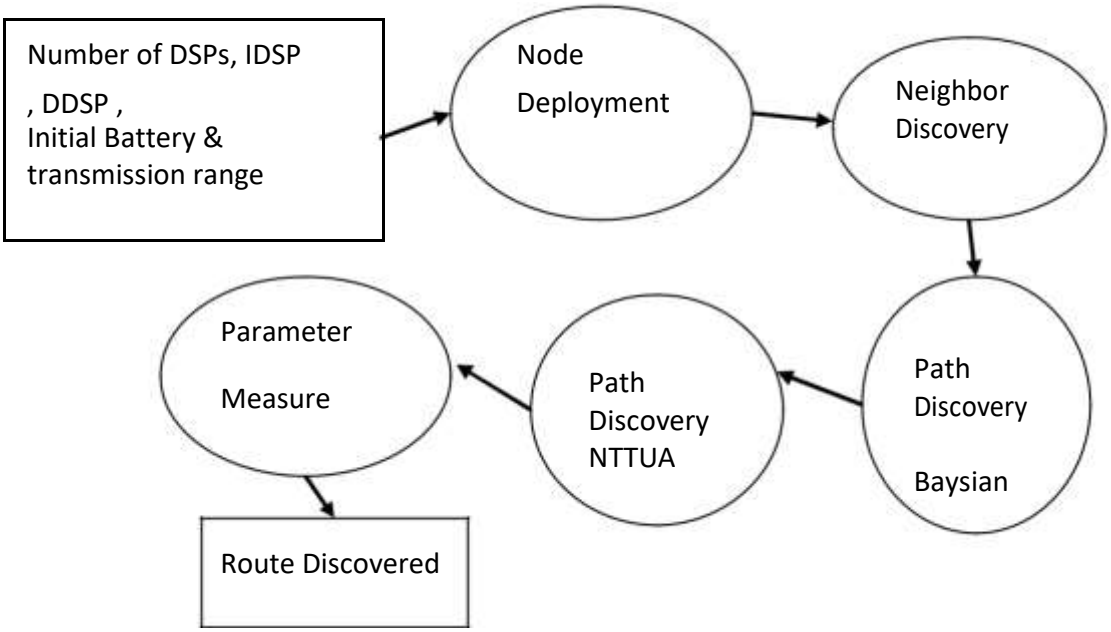

Fig 16: DFD Level 1

Fig 16 shows the DFD Level 1. The inputs for the DFD Level 1 are Number of DSPs, IDSP, DDSP, Initial Battery and Transmission Range. The process is sequence of operations namely Node Deployment, Neighbor Discovery, Path Discovery Baysian, Path Discovery NTTUA Approach, Parameter Measure. The Output is Path Discovered from IDSP to DDSP from the Baysian and NTTUA approach and its comparison.

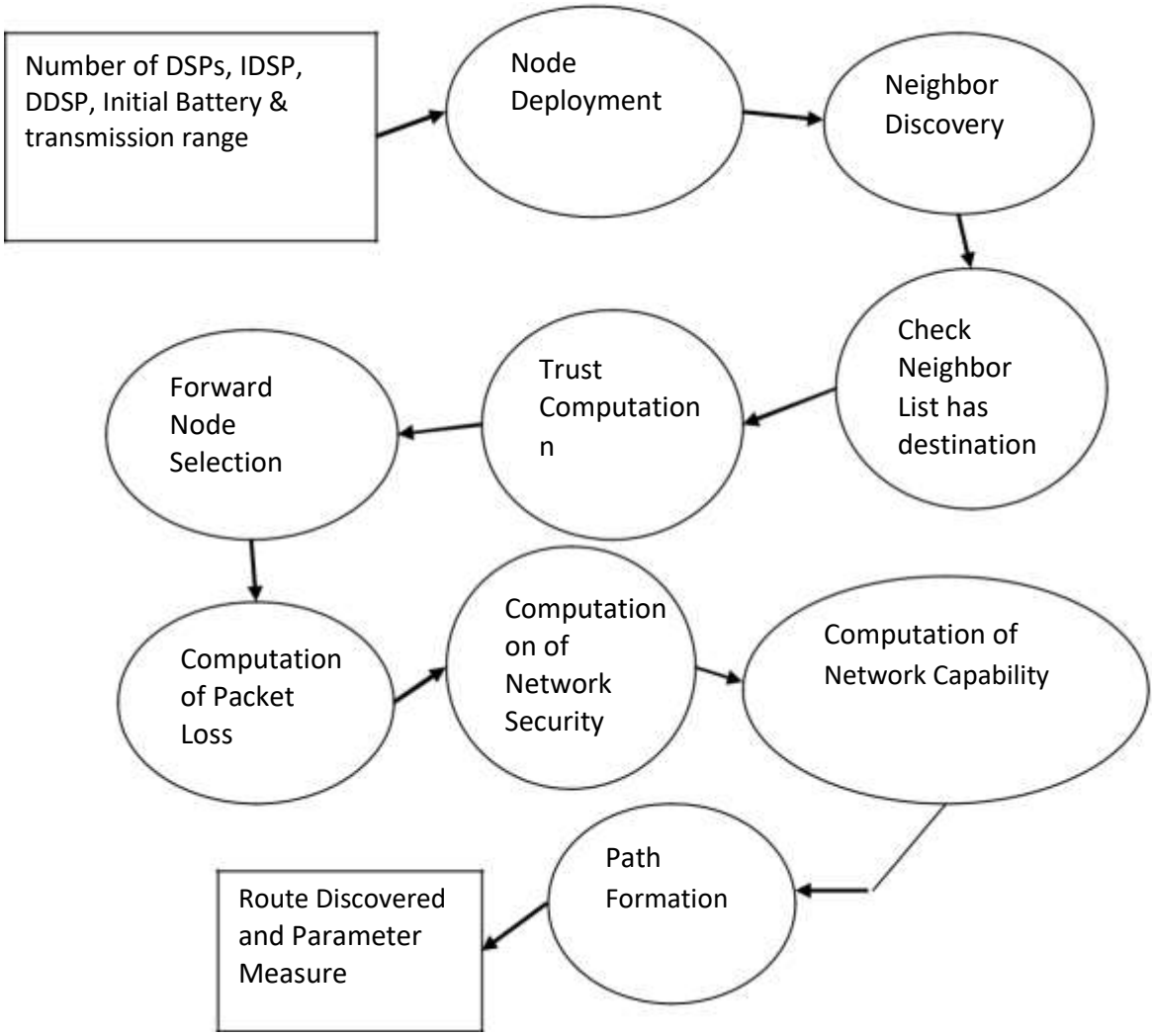

Fig 17: DFD Level2

Fig 17 shows even more in-depth information about DFD Level2. The inputs for the DFD Level 2 are Number of DSPs, IDSP, DDSP, Initial Battery and Transmission Range. The processes are sequence of operations namely Node Deployment, Neighbor Discovery, Check Neighbor contain destination, trust computation, forward node selection, computation of packet loss, network security, network capability and finally the path formation. The output is path discovered along with parameters measure.

4.4 DETAILED DESIGN

DSP Placement Algorithm

DSP placement Algorithm is the algorithm which is responsible for positioning the DSP in the network.

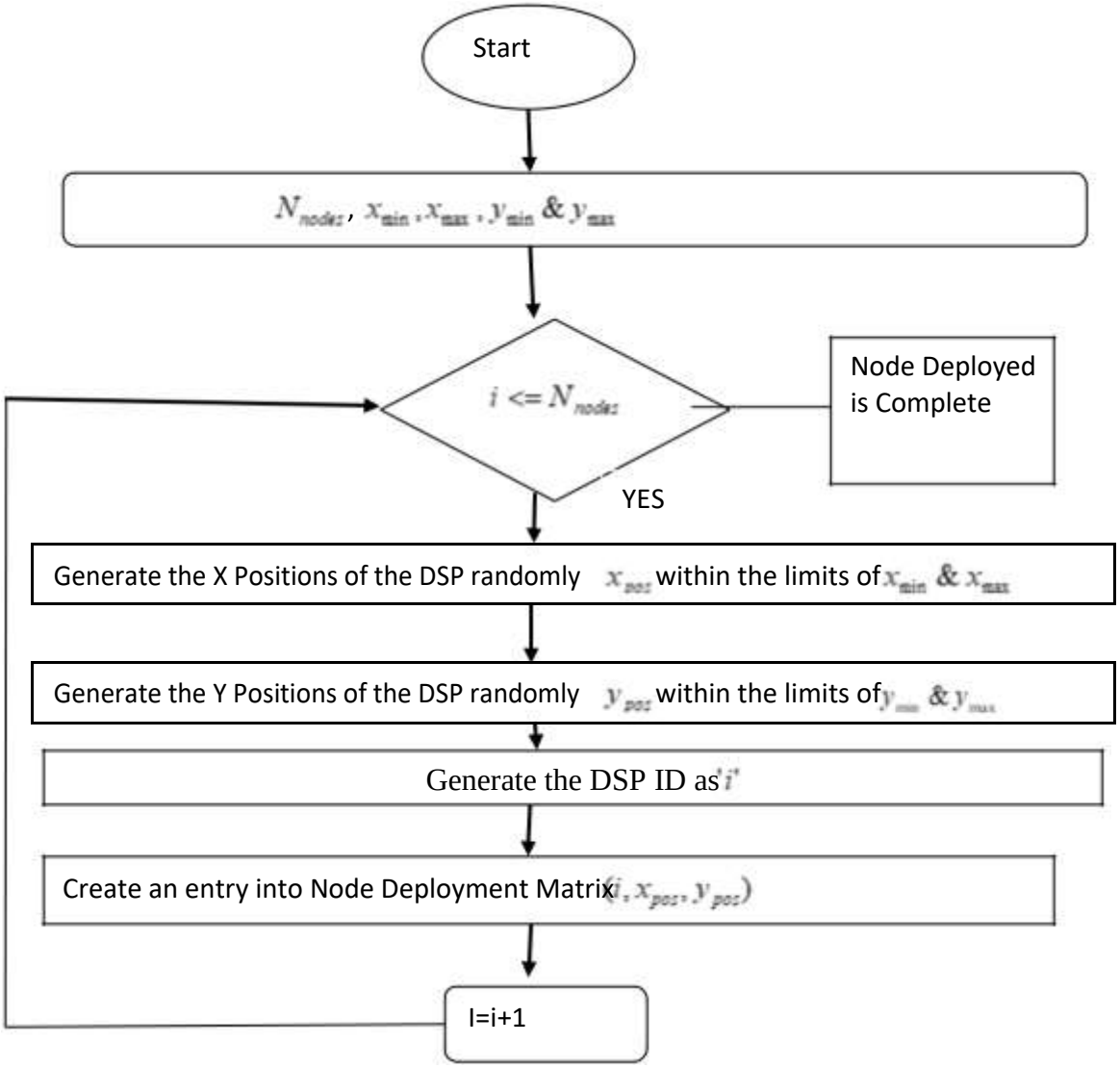

Fig 18: DSP Placement Algorithm

Fig 18 shows the DSP Deployment Algorithm which is responsible for placing the nodes in the network.

1. Number of DSPs, Minimum x position, Maximum x position, Minimum y position & Maximum y position will be the input.

2. Generate the DSP Id Starting with Node Id as '1'
3. Generate of X position of DSP randomly between x_{min} to x_{max}
4. Generate of Y position of DSP randomly between y_{min} to y_{max}
5. Store the information in the format of a set (i, x_{pos} , y_{pos})
6. Increment the DSP ID
7. Repeat the process until all nodes are placed in the network

Bayesian Method

The Bayesian Algorithm is used to find neighbors the route from the IDSP to DDSP.

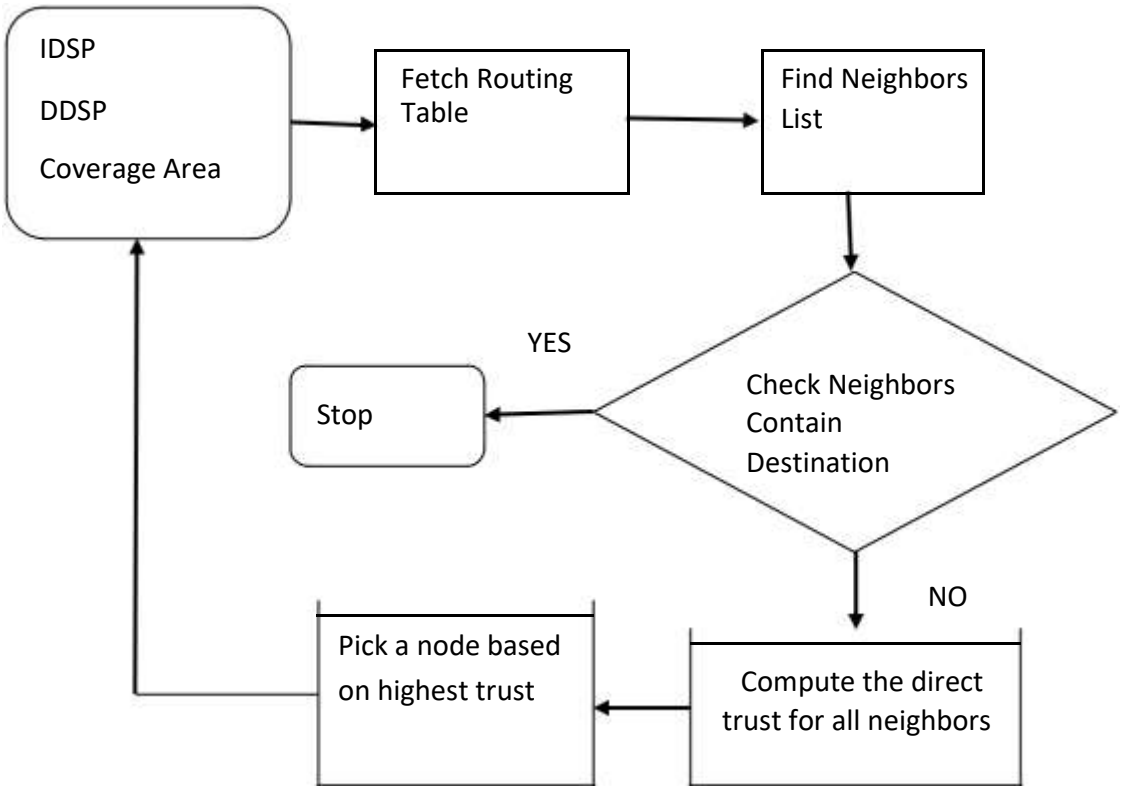

Fig 19: Baysian Trust Method

Fig 19 shows the flowchart for the Baysian Trust Method Algorithm.

1. IDSP, DDSP and Transmission Range acts as an input.
2. The IDSP will find the set of nodes within transmission range known as neighbor nodes.
3. If the neighbor nodes have the DDSP then stop the process.
4. If the neighbor nodes does not have the DDSP then compute the direct trust of each of the neighbor nodes based on Etx value.

$$TE_{tx} = \sum_{i=1}^{N} E_{txi} / N$$

$$E_{tx} = \frac{N_{ACK}}{N_{gen}}$$

5. Pick a node which has highest value of TE
6. Repeat process until DDSP is reached.

NTTUA algorithm

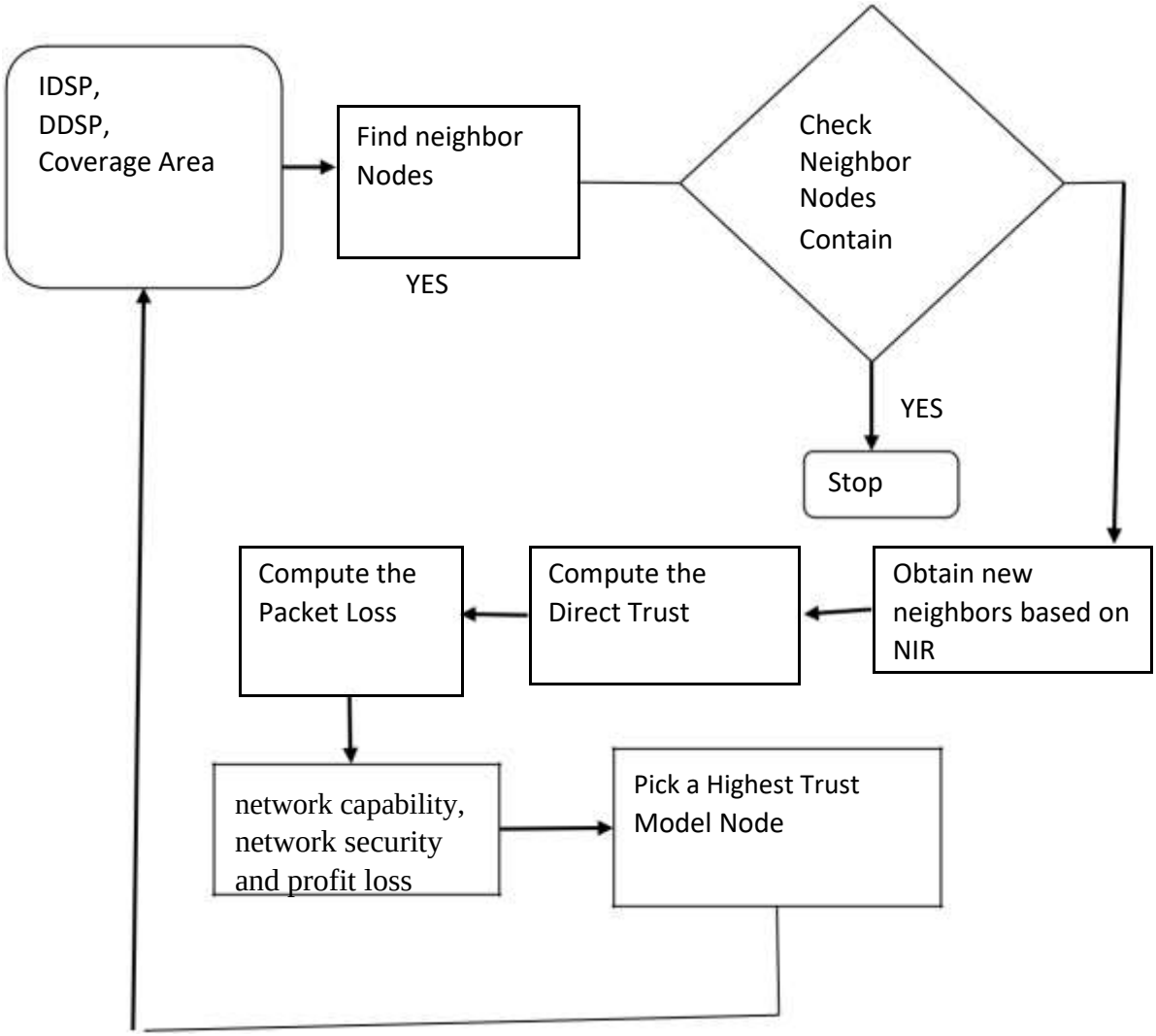

Fig 20: NTTUA Method

Fig 20 shows the flowchart for the proposed algorithm

1. IDSP, DDSP and Transmission Range acts as an input.
2. The Source Node will find the set of nodes within transmission range known as neighbor nodes.
3. If the neighbor nodes have the DDSP then stop the process.

4. If the neighbor nodes do not have the DDSP then compute the neighbor nodes using the NIR list
5. For the new neighbors find packet loss
6. For the new neighbors compute direct trust
7. For the new neighbor's compute network security, profit loss and network capability
8. Pick up a node which has the highest trust measure
9. Repeat process until destination is reached.

The packet loss can be computed as below

$$PL = Nsent - Nackrecieved$$

The network security is computed as below

$$NSI = 1 - \frac{Nineff}{Nnodes}$$

Nineff= Number of inefficient nodes in the transmission range of the node

Nnodes= Total Number of nodes in the transmission range

The Network Capability can be defined as

$$NC = \frac{NLI}{2 * NE}$$

Where,

NLI= average amount of data loss

NE=Total number of network edges

The Network Profit can be defined as follows

$$NP = mu1 * NSI + mu2 * NC$$

CHAPTER 5

IMPLEMENTATION

Use case diagrams

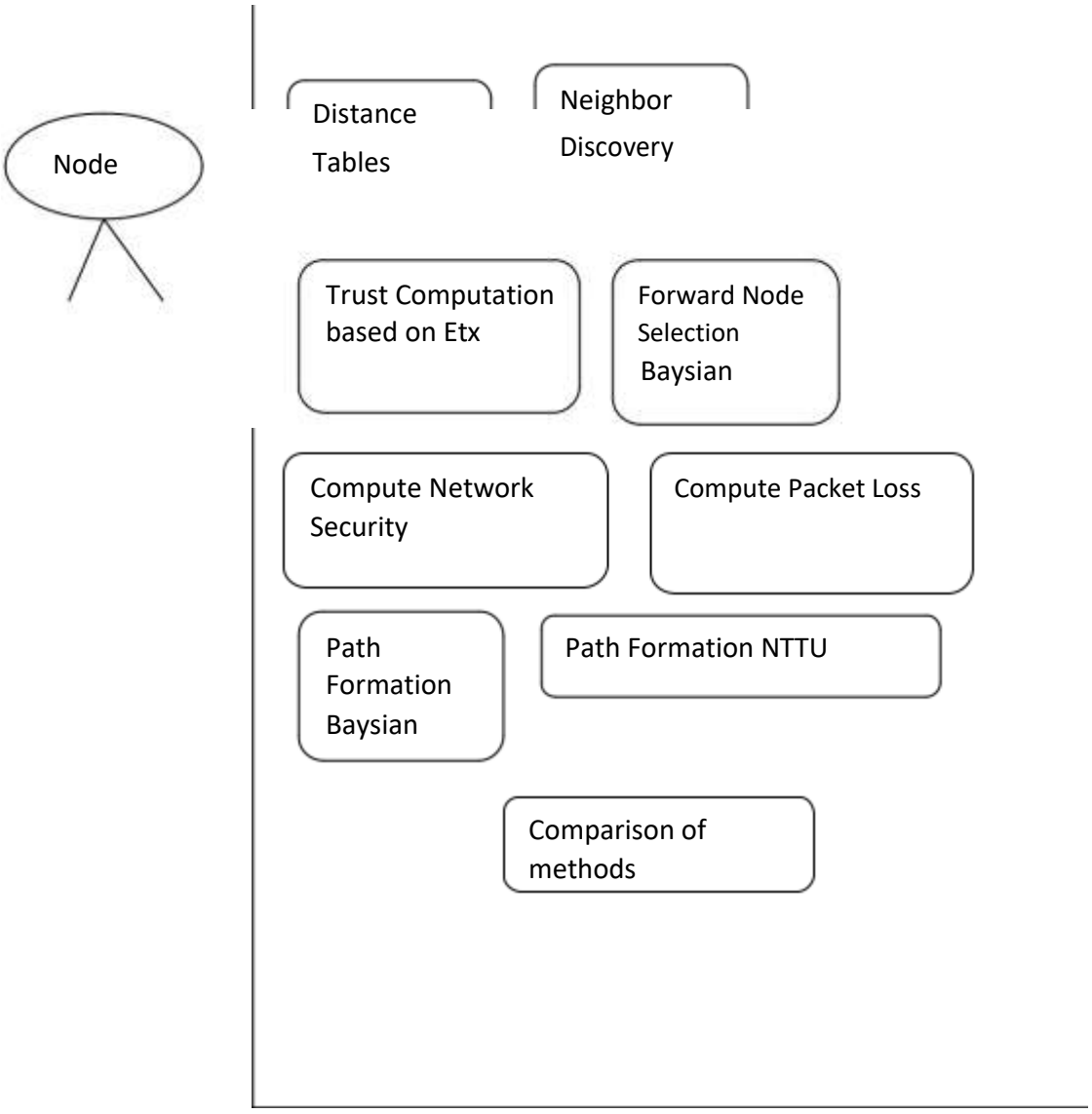

Fig 21: Use Case Diagram

The above figure 21 shows the actors and the various modules that the nodes will make use of for the complete execution of the project

Distance Tables

this table is used for the measurement of distance between the DSPs in the network.

Neighbor Discovery

This module is responsible for finding the DSPs which are within the transmission range

Trust Computation based on Etx

This module is responsible for computation of trust level based on the value of ETX which is computed using the following formula

$$TE_{tx} = \sum_{i=1}^{N} E_{txi} / N$$

$$E_{tx} = \frac{N_{ACK}}{N_{gen}}$$

Forward Node Selection Baysian

This module is responsible for selection of the node which has highest value for the Etx

Compute Network Security Index

This module is responsible for Network Security Index (NSI)

$$NSI = 1 - \frac{Nineff}{Nnodes}$$

Path Formation Baysian

The module is responsible for the computation of end to end path by making use of Etx value along with the other information. IDSP, DDSP and Transmission Range acts as an input. The IDSP will find the set of nodes within transmission range known as neighbor nodes. If the neighbor nodes have the DDSP then stop the process. If the neighbor nodes do not have the DDSP, then compute the direct trust of each of the

neighbor nodes based on Etx value. $TE_{tx} = \sum_{i=1}^{N} E_{txi} / N$ and $E_{tx} = \frac{N_{ACK}}{N_{gen}}$ Pick a node which has

highest value of TE and Repeat process until DDSP is reached

Path Formation NTTU

The Path Formation for NTTU can be defined as IDSP, DDSP and Transmission Range acts as an input. The Source Node will find the set of nodes within transmission range known as neighbor nodes. If the neighbor nodes have the DDSP then stop the process. If the neighbor nodes do not have the DDSP then compute the neighbor nodes using the NIR list - For the new neighbors find packet loss, For the new neighbors compute direct trust, For the new neighbors compute network security, profit loss and network capability and Pick up a node which has the highest trust measure. Repeat process until DDSP is reached.

Comparison of methods

The various parameters are compared between the proposed method and the existing baysian based trust approach with respect to time taken, link count, total path energy utilization, residual energy, number of efficient nodes, number of non-efficient nodes, lifetime ratio, routing overhead and throughput.

5.1 FUNCTIONS BAYSIAN APPROCH

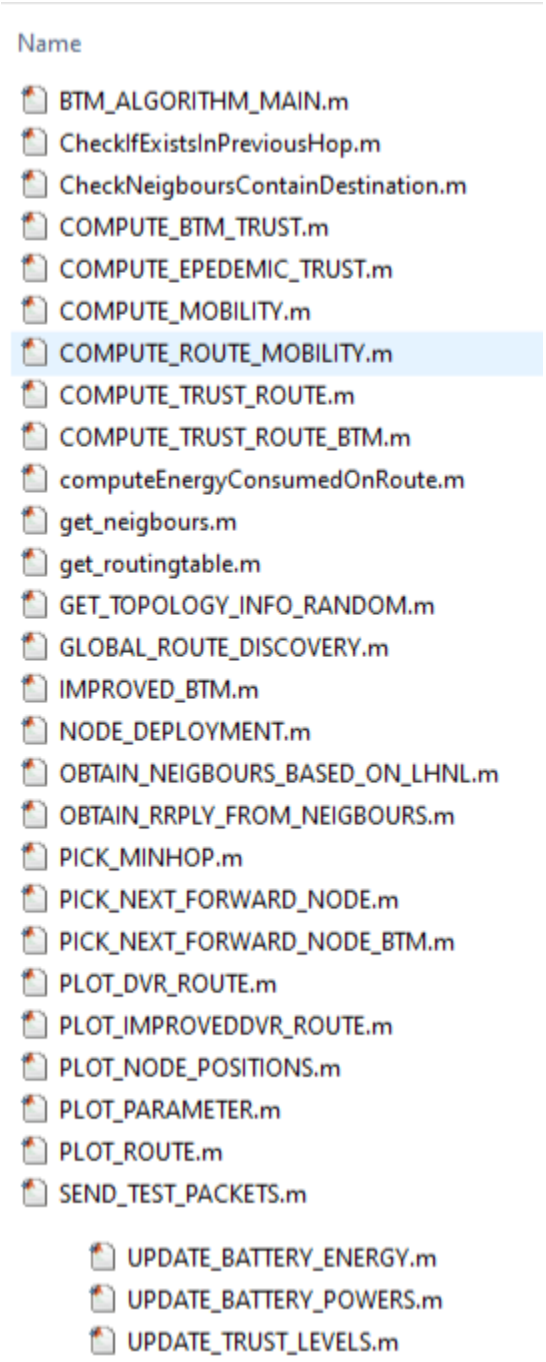

Fig 22: Baysian Trust Method Class Diagram

The following is the table describes the various ramifications used in the implementation of previous approach

Name	**Description**
BTM_ALGORITHM_MAIN	end to end flow of the algorithm can be executed using this ramification Bayesian Trust Method
calculate_distance	The ramification is used to compute the distance between the DSPs
CheckIfExistsInPreviousHop	This ramification is used to check whether the currently picked DSP was present in previous hop of the path or not
CheckNeigboursContainDestination	check whether neighbors has DDSP. if yes, the ramification returns true otherwise it returns false
COMPUTE_BTM_TRUST	This ramification is responsible for the computation of Baysian Trust for the entire route
COMPUTE_DISTANCE_WRT_CENTER	This ramification is used to compute the distance with respect to Given location point
COMPUTE_EPEDIMIC_TRUST	This is used to compute the trust for the overall path
COMPUTE_MOBILITY	This ramification is responsible for computing the mobility of nodes in the network.
COMPUTE_ROUTE_MOBILITY	Changing the location of DSPs after certain period of time i.e entire DSPs which are participating in routing
COMPUTE_TRUST_ROUTE	This ramification computes the trust level for the entire route by performing the summation of all nodes trust in the route.

COMPUTE_TRUST_ROUTE_BTM	This ramification computes the trust level for the entire route by performing the summation of all nodes trust in the route.
GLOBAL_ROUTE_DISCOVERY	This is used to find all possible paths between the given source node to destination node
computeDistance	The distance between DSP1 and DSP2 is computed using this ramification
computeEnergyConsumedOnRoute	For a given transmission energy, generation energy, distance between DSPs and attenuation factor this will compute the energy consumption
IMPROVED_BTM	This ramification is responsible for path discovery between IDSP to DDSP by first finding the DSPs within transmission range, computing the trust for the DSPs , picking the DSP with high value of trust and then updating the battery levels for the DSPs
OBTAIN_NEIGBOURS_BASED_ON_LHNL	This ramification is responsible for finding the neighbor nodes by making use of last hop neighbor list
OBTAIN_RRPLY_FROM_NEIGBOURS	This ramification is responsible for obtaining the REPLY from the nodes which are within the transmission range
PICK_MINHOP	This ramification is responsible for finding the path efficiently once the threshold hops are reached
PICK_NEXT_FORWARD_NODE	This ramification is responsible for picking the node which has the highest trust

PICK_NEXT_FORWARD_NODE_ BTM	This ramification is responsible for picking the node which has the highest trust
SEND_TEST_PACKETS	This ramification is responsible for sending the test packets to the end user and then obtain the reply for the sent test packets

computeNoOfEffcientNodes	This ramification is used to compute the number of Efficient nodes in the network by taking the remaining battery energy levels of the nodes
computeNoOfDeadNodes	This ramification is used to compute the number of dead nod es in the network by taking the remaining battery energy levels of the nodes
CORRECT_ROUTE_LAST_INDE X	The ramification is used to append the destination node in the control packet
FIND_DEAD_NODES	This ramification is used to find the dead nodes in the network
FIND_DISTANCE	This ramification is responsible for computing the distance between the nodes
findMatrix	This ramification is used to check whether neighbor exists in route
get_neigbours	This ramification is used to obtain the neighbor list from the routing table
get_routingtable	This ramification is used to find the routing table for the specific node in the network
GET_TOPOLOGY_INFO_RANDO M	This ramification is responsible for generating routing tables for all nodes in the network
NODE_DEPLOYMENT	This ramification is responsible for generating the position of nodes in the network based on end points and the number of nodes

OBTAIN_NEIGBOURS_BASED_ ON_NIR	This ramification is used to remove the nodes which have been already in the route and generate new neighbors which has not traversed
PICK_DISTANCE	This ramification is used to find the nodes which are closer to the destination node and pick a node closer to destination node

PICK_MINHOP	This ramification is used to pick the nodes which are closest to destination. This works on Minimum hop algorithm
PLOT_NODE_POSITIONS	This ramification is used to plot the nodes in the network for a given cross-sectional area
PLOT_ROUTE	This ramification is used to plot the network and then plot the route between source node and destination node
removeNodesAlreadyGoneThrough	This ramification is used to remove the nodes which have been traversed
UPDATE_BATTERY_ENERGY	This ramification is used to update the energy levels of the nodes which participates in the network

TABLE 13: Functions Baysian approach

5.2 FUNCTION DIAGRAM FOR PROPOSED METHOD

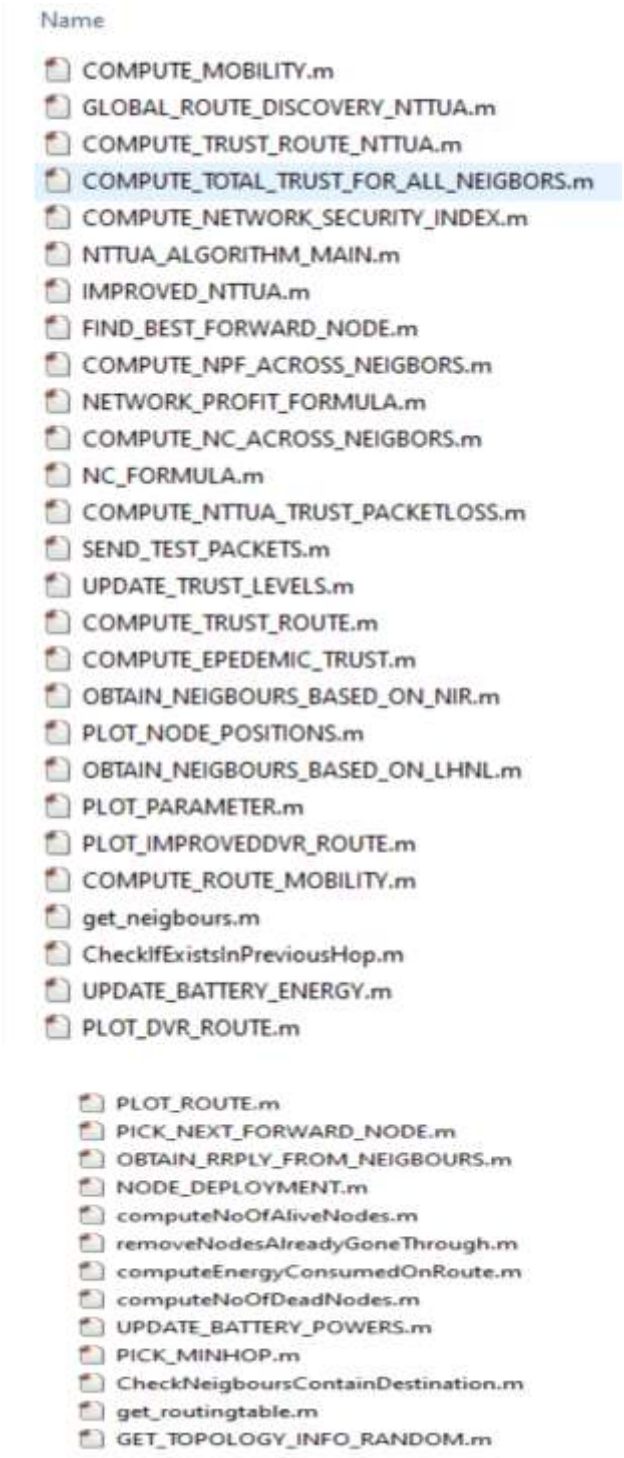

Fig 23: NTTUA Method

Ramification Name	Ramification Description
NTTUA_ALGORITHM_MAIN	This ramification is used to execute the end to end flow of proposed method starting from network formation, find the nodes within the transmission range, compute the end to end route, update the remaining energy levels for all the nodes in the network
GLOBAL_ROUTE_DISCOVERY_ NTTUA	This ramification is responsible for finding all possible paths from the initiators till the destination node in the network. Starting from the first node till the number of nodes in the network path is found between each initiator node to destination node. After that this ramification will also compute the total trust for each paths and then pick the path which is having highest trust is also found in this ramification, The ramification future computes the mobility of the route as well as average mobility along with variance mobility
COMPUTE_TRUST_ROUTE_NTT UA	This ramification is responsible for finding the overall trust for the entire path between source to destination node
COMPUTE_TOTAL_TRUST_FOR _ALL_NEIGBORS	This ramification is responsible for computing the total trust for each neighbor node based on number of Negative Acknowledgements, direct value of trust computation
IMPROVED_NTTUA	This ramification is responsible for the finding the end to end path between source node to destination node. First the initiator will find the neighbors, compute the neighbors trust dependent on multiple factors and then pick the node with highest trust and then finally repeat process until destination is reached
COMPUTE_NETWORK_SECURI	This ramification will find the in-efficient nodes and then compute

calculate distance	The ramification is used to compute the distance between the nodes
CheckIfExistsInPreviousHop	This ramification is used to check whether the currently picked neighbor was present in previous hop of the route
CheckNeigboursContainDestination	The ramification is used to check whether neighbors has destination node. if yes, the ramification returns 1 otherwise it returns a 0
COMPUTE_DISTANCE_WRT_CE NTER	This ramification is used to compute the distance with respect to reference point
COMPUTE_EPEDIMIC_TRUST	This is used to compute the trust for the overall path
COMPUTE_MOBILITY	This ramification is responsible for computing the mobility of nodes in the network.
COMPUTE_ROUTE_MOBILITY	This ramification is responsible for computing the mobility of the entire nodes which are participating in routing
COMPUTE_TRUST_ROUTE	This ramification computes the trust level for the entire route by performing the summation of all nodes trust in the route.
COMPUTE_TRUST_ROUTE_BT M	This ramification computes the trust level for the entire route by performing the summation of all nodes trust in the route.
GLOBAL_ROUTE_DISCOVERY	This is used to find all possible paths between the given source node to destination node
compute Distance	This ramification is used to compute the distance between the nodes in the network
computeEnergyConsumedOnRoute	This ramification contains the implementation formula for energy consumption for the route

OBTAIN_NEIGBOURS_BASED_ON_LHNL	This ramification is responsible for finding the neighbor nodes by making use of last hop neighbor list
OBTAIN_RRPLY_FROM_NEIGBOURS	This ramification is responsible for obtaining the REPLY from the nodes which are within the transmission range
PICK_MINHOP	This ramification is responsible for finding the path efficiently once the threshold hops are reached
PICK_NEXT_FORWARD_NODE	This ramification is responsible for picking the node which has the highest trust
PICK_NEXT_FORWARD_NODE_BTM	This ramification is responsible for picking the node which has the highest trust
SEND_TEST_PACKETS	This ramification is responsible for sending the test packets to the end user and then obtain the reply for the sent test packets
computeNoOfEffcientNodes	This ramification is used to compute the number of Efficient nodes in the network by taking the remaining battery energy levels of the nodes
computeNoOfDeadNodes	This ramification is used to compute the number of dead nodes in the network by taking the remaining battery energy levels of the nodes
CORRECT_ROUTE_LAST_INDEX	The ramification is used to append the destination node in the control packet
FIND_DEAD_NODES	This ramification is used to find the dead nodes in the network
FIND_DISTANCE	This ramification is responsible for computing the distance between the nodes
findMatrix	This ramification is used to check whether neighbor exists in route

get_neigbours	This ramification is used to obtain the neighbor list from the routing table
get_routingtable	This ramification is used to find the routing table for the specific node in the network
GET_TOPOLOGY_INFO_RANDOM	This ramification is responsible for generating routing tables for all nodes in the network
NODE_DEPLOYMENT	This ramification is responsible for generating the position of nodes in the network based on end points and the number of nodes
OBTAIN_NEIGBOURS_BASED_ON_NIR	This ramification is used to remove the nodes which have been already in the route and generate new neighbors which has not traversed
PICK_DISTANCE	This ramification is used to find the nodes which are closer to the destination node and pick a node closer to destination node
PICK_MINHOP	This ramification is used to pick the nodes which are closest to destination. This works on Minimum hop algorithm
PLOT_NODE_POSITIONS	This ramification is used to plot the nodes in the network for a given cross-sectional area
PLOT_ROUTE	This ramification is used to plot the network and then plot the route between source node and destination node
removeNodesAlreadyGoneThrough	This ramification is used to remove the nodes which have been traversed
UPDATE_BATTERY_ENERGY	This ramification is used to update the energy levels of the nodes which participates in the network

Table 14: Function Diagram for NTTUA method

CHAPTER 6

TESTING

There are multiple kind of testing which are involved for the algorithms, in this section in order to test for the complete work we need to test each individual module functionality and hence unit test cases help in identifying whether the algorithms produce desirable results.

6.1 Unit Test Cases

This chapter describes the list of test cases executed in the project

Test Case ID	Test1
Test Description	Generation of DSP Deployment Matrix
Input	Number Of DSPs. Distance Between the DSPs, Battery Level of Nodes
Expected Output	DSPs location and unique identifier for specified number of DSPs
Actual Output	DSPs location and unique identifier for specified number of DSPs
Test Result	PASS

Table 15: DSP Deployment Algorithm

Test Case ID	Test2
Test Description	Generation of Distance Tables
Input	Deployment Info
Expected Output	Distance Tables getting generated for specified number of DSPs
Actual Output	Distance Tables getting generated for specified number of DSPs
Test Result	PASS

Table 16: Distance Table Generation Test

Test Case ID	Test3
Test Description	Find route from IDSP to DDSP using BAYSIAN METHOD
Input	IDSP & DDSP
Expected Output	Path from IDSP to DDSP using BAYSIAN METHOD
Actual Output	Route from IDSP to DDSP using BAYSIAN METHOD
Test Result	PASS

Table 17: Path Discovery Algorithm BAYSIAN METHOD

Test Case ID	Test5
Test Description	Find route from source node to destination node using NTTUA METHOD
Input	Source node & destination Node
Expected Output	Route from source node to destination node using NTTUA METHOD
Actual Output	Route from source node to destination node using NTTUA METHOD
Test Result	PASS

Table 18: Path Discovery Algorithm NTTUA METHOD

Test Case ID	Test6
Test Description	Comparison with BAYSIAN and NTTUA METHOD End to End Delay
Input	IDSP, DDSP, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	End to End Delay is lowest for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	End to End Delay is lowest for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 19: Comparison with BAYSIAN METHOD and NTTUA METHOD – End to End Delay

Test Case ID	Test7
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD Number of Hops
Input	IDSP, DDSP, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Number of Hops is lowest for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Number of Hops is lowest for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 20: Comparison with BAYSIAN METHOD and NTTUA METHOD – Number of Hops

Test Case ID	Test8
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD Total Energy Consumption
Input	Source nod, destination Node, TTL, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Total Energy Consumption is lowest for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Total Energy Consumption is lowest for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 21: Comparison with BAYSIAN METHOD and NTTUA METHOD – Total Energy Consumption

Test Case ID	Test9
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD Number of Efficient Nodes
Input	Source nod, destination Node, TTL, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Number of Efficient Nodes are higher for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Number of Efficient Nodes are higher for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 22: Comparison with BAYSIAN METHOD and NTTUA METHOD – Number of Efficient Nodes

Test Case ID	Test10
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD Number of Dead Nodes
Input	Source nod, destination Node, TTL, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Number of Dead Nodes are less for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Number of Dead Nodes are less for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 23: Comparison with BAYSIAN METHOD and NTTUA METHOD – Number of Dead Nodes

Test Case ID	Test11
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD - Routing Overhead
Input	Source nod, destination Node, TTL, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Routing Overhead is less for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Routing Overhead is less for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 24: Comparison with BAYSIAN METHOD and NTTUA METHOD – Routing Overhead

Test Case ID	Test12
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD - Lifetime Ratio
Input	Source nod, destination Node, TTL, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Lifetime Ratio is more for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Lifetime Ratio is more for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 25: Comparison with BAYSIAN METHOD and NTTUA METHOD – Lifetime Ratio

Test Case ID	Test13
Test Description	Comparison with BAYSIAN METHOD and NTTUA METHOD - Throughput
Input	Source nod, destination Node, TTL, Transmission Range, Energy required for Transmission, Energy required for Amplification, Attenuation Factor, Initial Energy
Expected Output	Throughput is more for NTTUA METHOD as compared to BAYSIAN METHOD
Actual Output	Throughput is more for NTTUA METHOD as compared to BAYSIAN METHOD
Test Result	PASS

Table 26: Comparison with BAYSIAN METHOD and NTTUA METHOD – Throughput

CHAPTER 7

RESULTS

In the current trust methods, the Initiator Data Sensing Point (IDSP) and Destination Data Sensing Point (DDSP) along with the transmission distance will act as input, The SPs which are within transmission range are found out. If the SPs have the DSP, then the process is stopped. Otherwise the next SP for the path is chosen based on trust computation which depends on the aggregation ratio of packet acknowledgement rate is computed within the transmission range and then the next SP which corresponds to highest value of aggregated ratio is chosen. The process is repeated until the DSP is reached. The various disadvantages of the current process are as follows- first is selecting the DSPs depends on the aggregated ratio process which is time consuming, secondly During the selection of DSPs since there is no trace maintained along the path there is high probability of back and forth propagation which leads to more number of hops and thirdly the energy consumption for the path can be computed as the aggregation of all the link energy across the path which is more and hence increases the number of dead data sense points. The research proposal will make use of trace list which prevents back and forth propagation between DSPs as the entire DSP list is appended to the control packet. The selection criteria for DSP will be improved by making use of multiple factors for the SPs within the transmission distance those include computes efficient data sense points, profit loss function along with Sensing Field capability. Eventually when the existing method is compared with the research proposal with respect to delay, energy consumption, in-efficient data sense points the proposal will perform in a better fashion.

This section will describe the experimental results

The input used in the algorithm's implementation using MATLAB can be described as below

Name	Value
Number of DSPs	100
Initial Level of Energy for SPs	3000 mJ
Number of Experimental Iterations	100
IDSP	4
DDSP	18
Coverage Area	40 m
Energy Required for data packet send	20 mJ
Energy Required for data packet generate	10 mJ
Attenuation factor	0.5

Table 27: Experimental Set Up Baysian

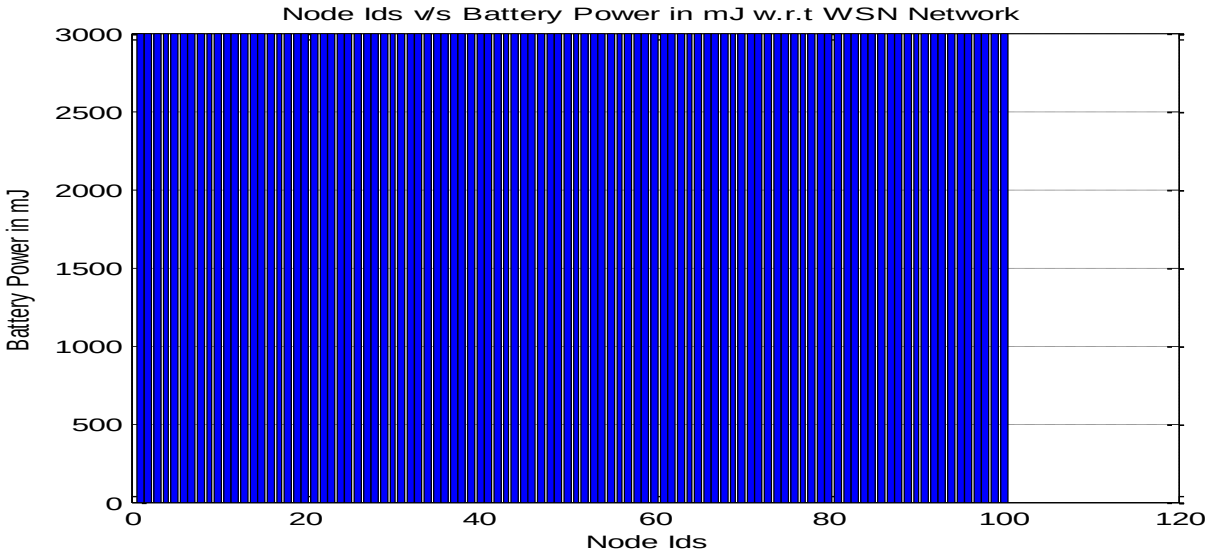

Fig 24: Battery Initialization for the Data sense points

Fig shows the battery initialization for the data sense points. As shown in the fig there are 100 data sense points and all the 100 data sense points are initialized with the same amount of battery power of about 3000 mJ.

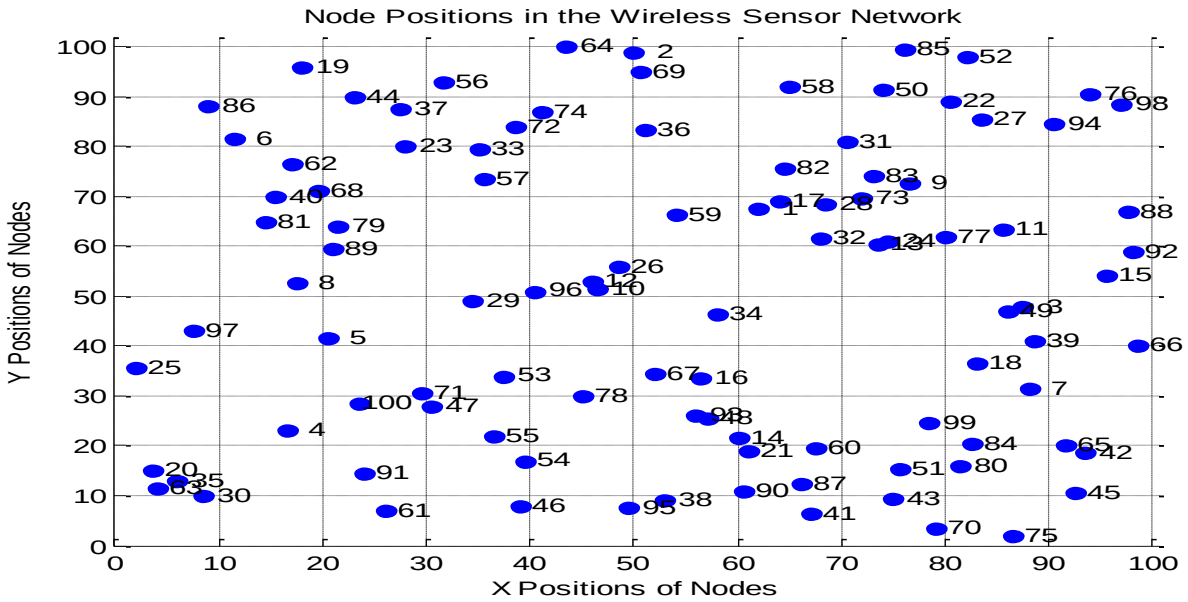

Fig25: Data sense points Distribution Algorithm

Fig25 shows the data sense points distribution algorithm, As shown in the fig there are 100 data sense points in the Sensing Field. Each data sense points are spread within an area of 100 * 100 meters. The data sense points positions are unique to each other. Data sense points 30 is placed at (10,10) , Data sense points 75 is placed at (88,2). In a similar fashion all remaining data sense pointss are placed in the Sensing Field

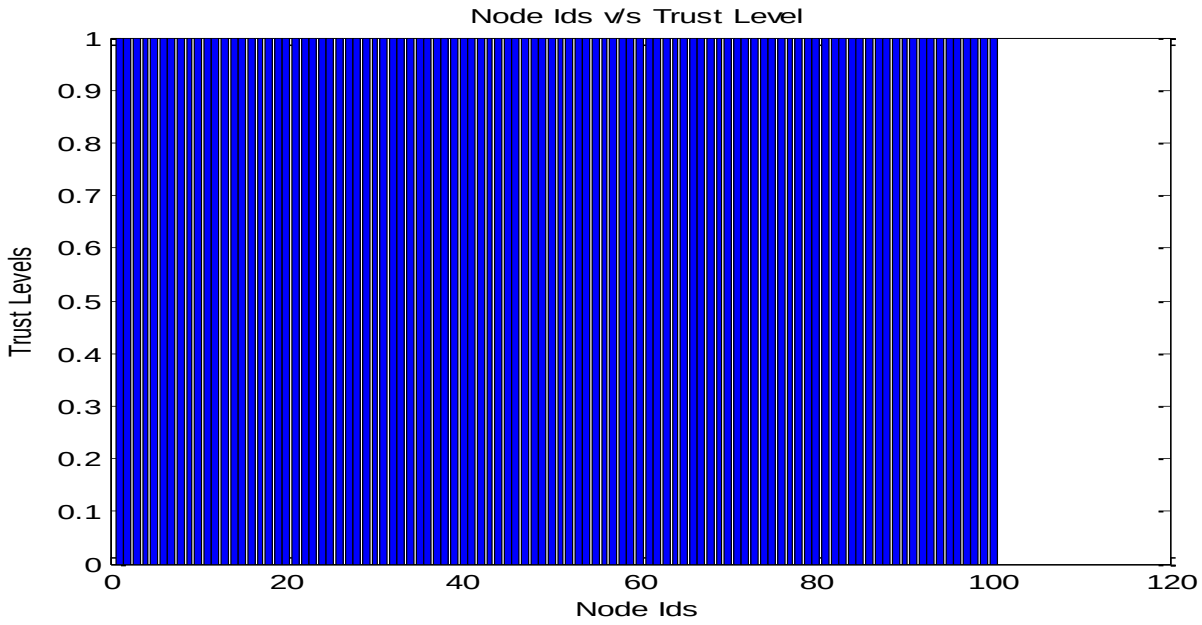

Fig26: Trust Level

Fig shows the trust level for the data sense points. All the 100 data sense points have the same amount of trust with a value of 1.

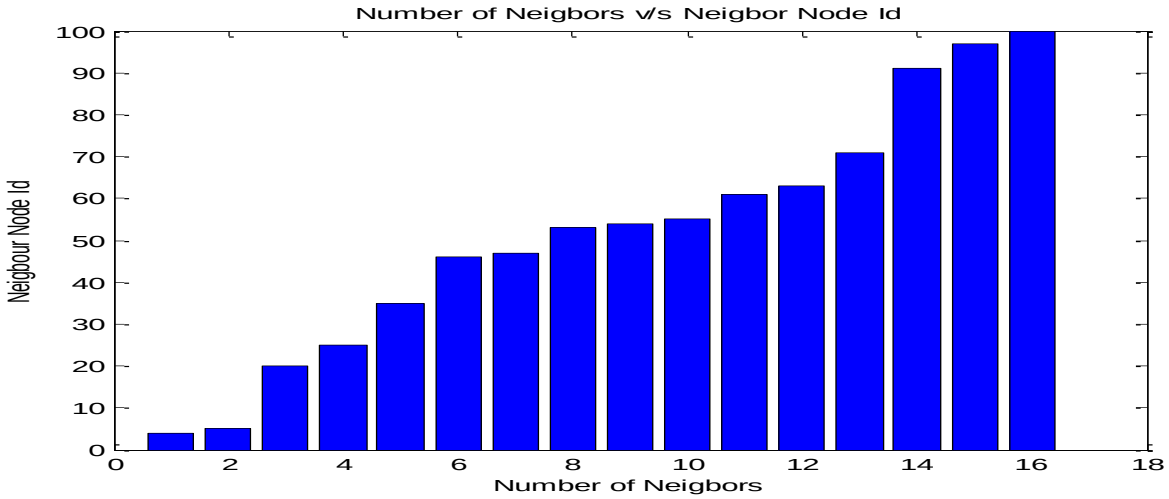

Fig27: Number of Neighbors

Fig shows the number of neighbors. As shown in the fig there are 16 data sense points which are neighbors of the initiator.

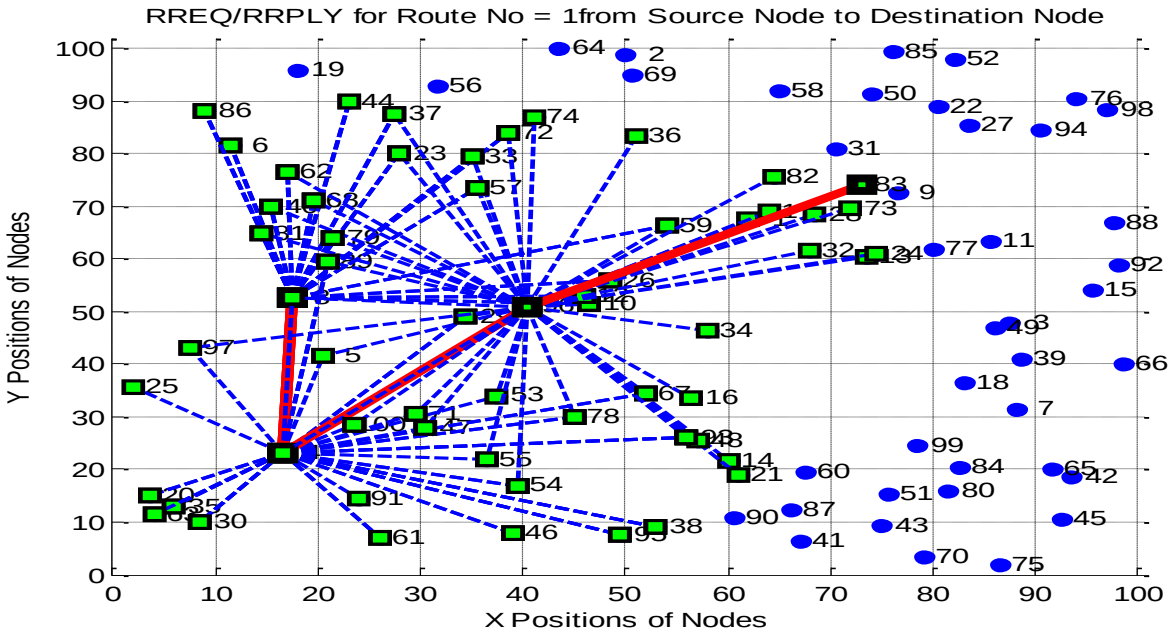

Fig 28: Path 1 from IDSP to DDSP

Fig 28 shows the route number 1 in which the blue color is the RREQ and then red color is an indication of RPLY which can be send back to the data sense points.

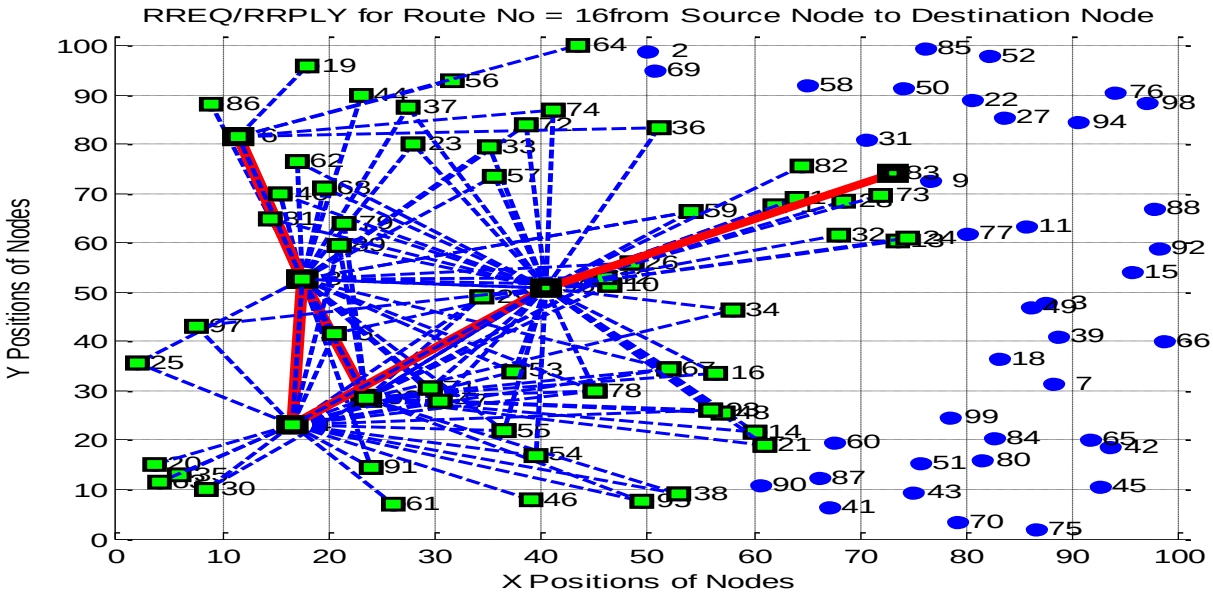

Fig29: Path No 16 from IDSP to DDSP

Fig29 shows the path number 16. From the source data sense points the RREQ/RRPLY is indicated between the source and destination data sense points.

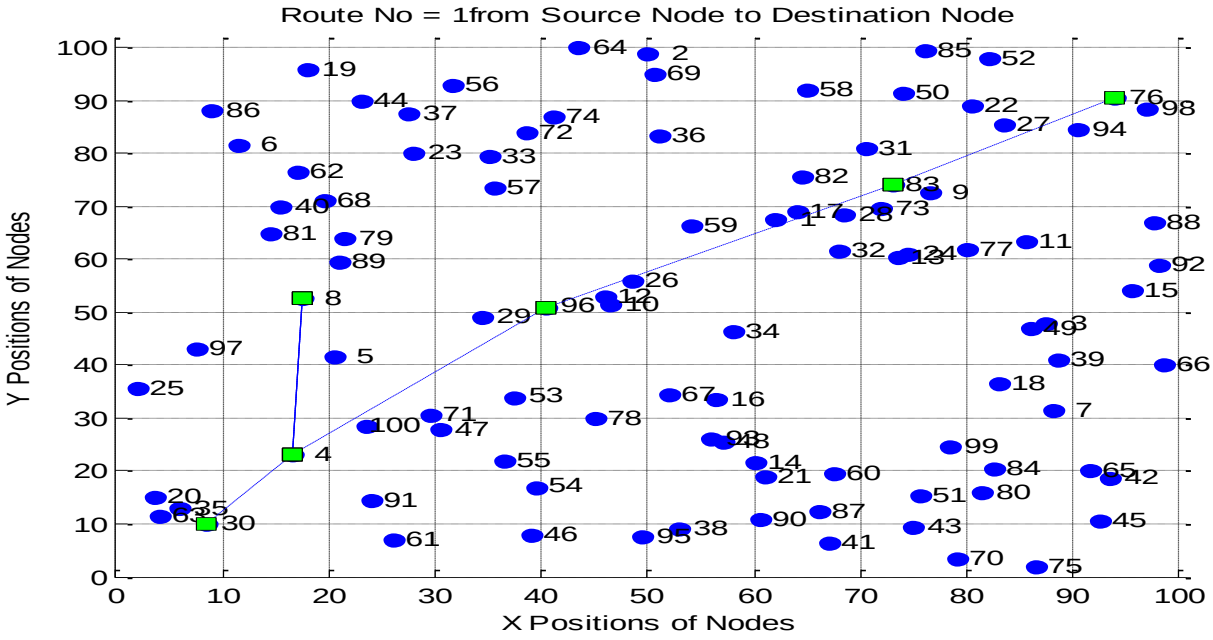

Fig30: Path1 from source data sense points to destination data sense points

Fig 30 shows the path number 1 from the initiator data sense points of Data sense points30 to destination data sense points 76.

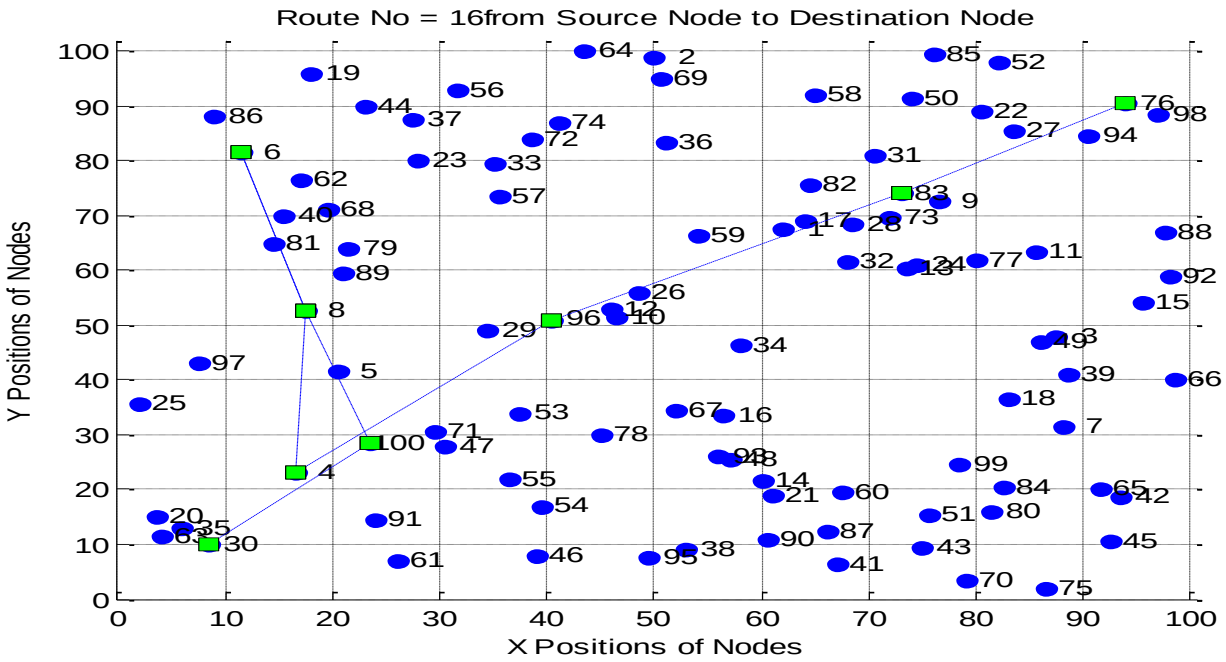

Fig31: Route 16 from IDSP to DDSP

Fig 31 shows the route between IDSP to DDSP in the Sensing Field. The initiator is DSP 30 and then the destination DSP is 76.

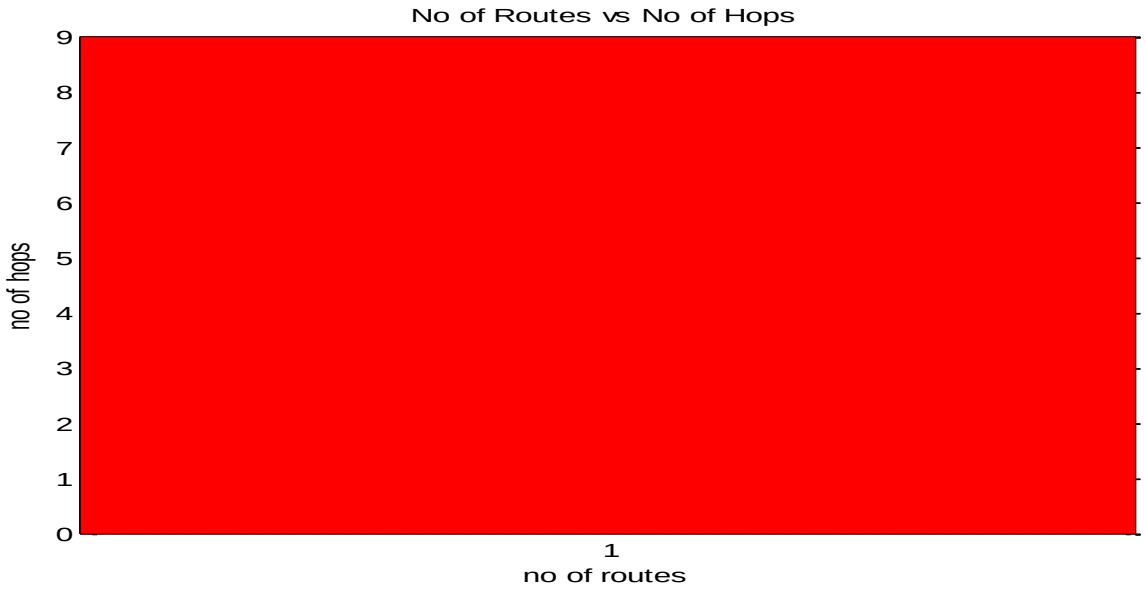

Fig 32: Hops Measure

Fig 32shows the hops for the best route in the Sensing Field. As shown in the fig there are overall 9 hops in the Sensing Field.

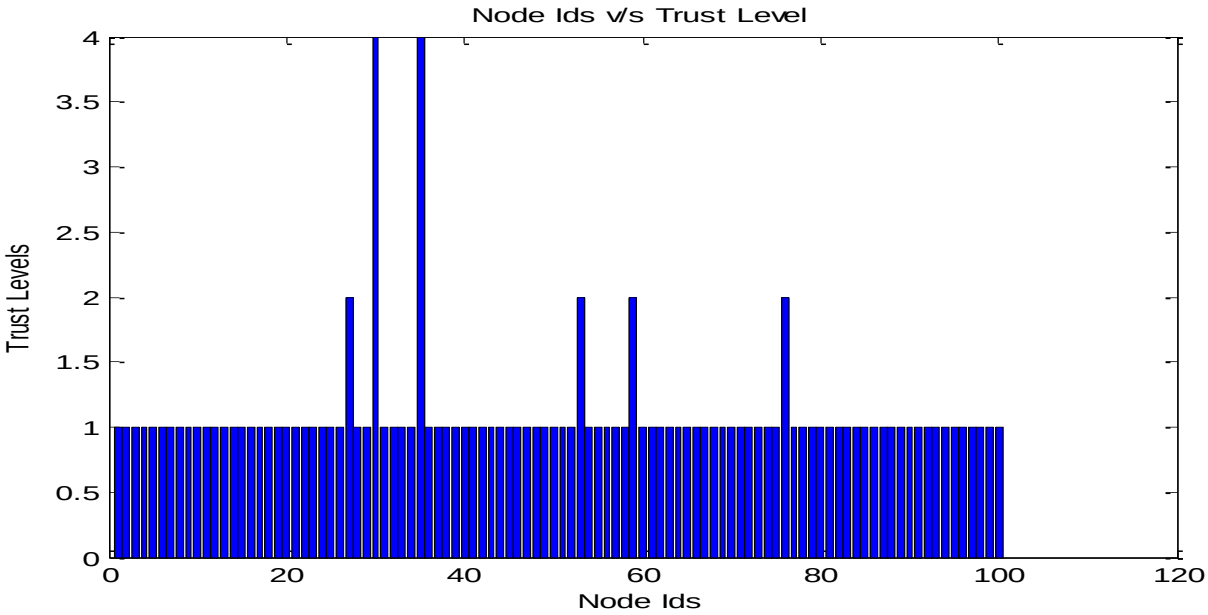

Fig 33: Trust Level Measure

Fig33 shows the trust level measure for the various data sense points in the Sensing Field. As shown in the fig there are 100 data sense points. The data sense points which are in the best path are having their trust level improved as compared to earlier value.

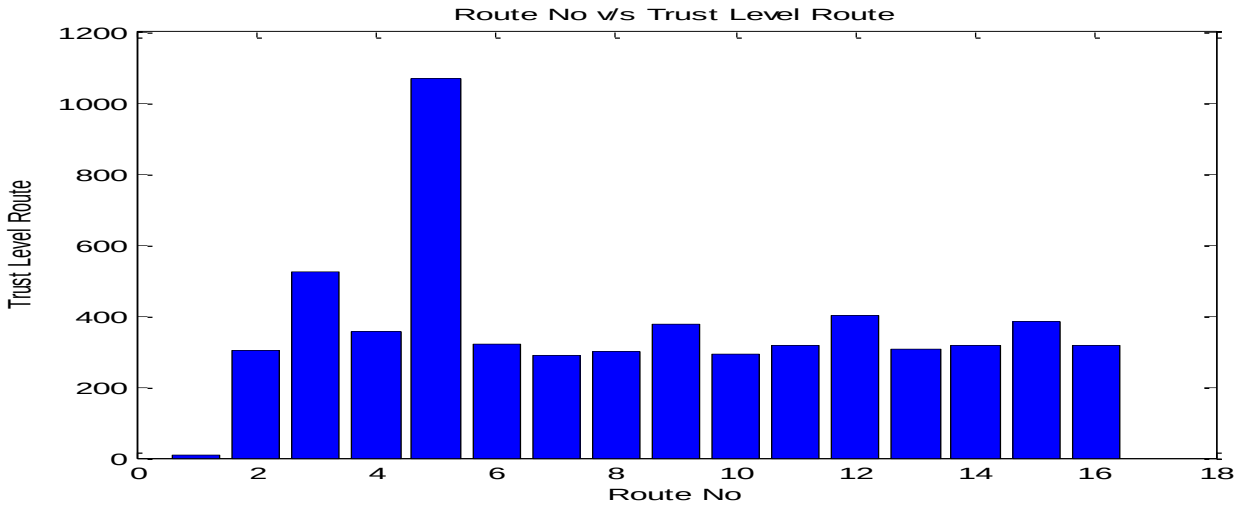

Fig 34: Paths v/s Trust Levels

Fig 34 shows the paths with the trust levels on the vertical axis. As shown in the fig there are 16 paths and the corresponding trust level is represented in the vertical axis. From the fig once can see that path 5 has the highest trust level and hence can be treated as the best path.

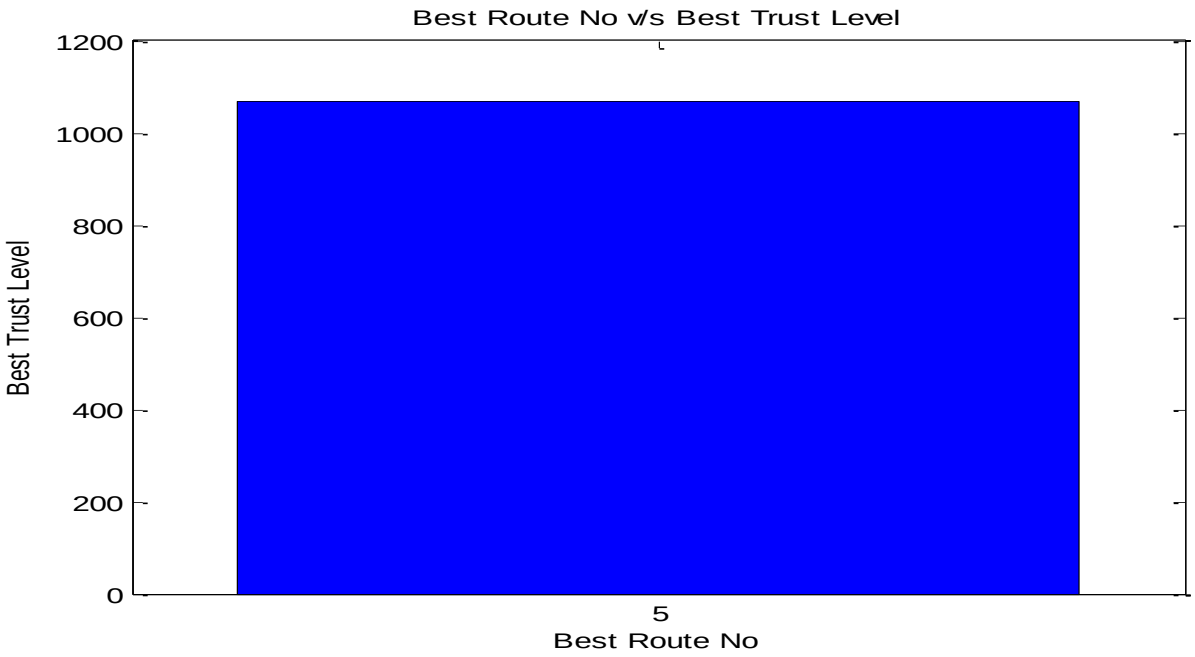

Fig 35: Best Route No

Fig35 shows the best route to be route number and the corresponding trust value to be higher

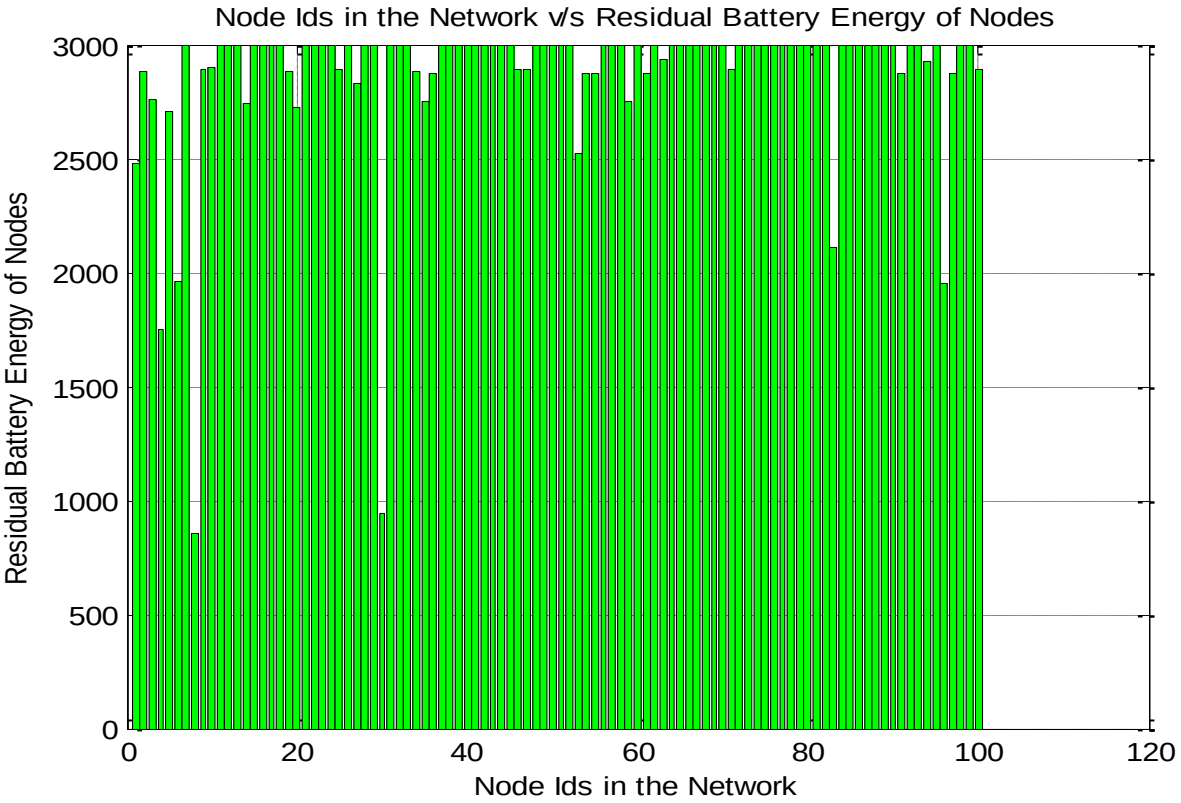

Fig36: Residual Battery Energy for the Data sense points

Fig36 shows the residual battery energy for the data sense points in the Sensing Field. As shown in the fig there are 100 data sense points in the Sensing Field and the data sense points which

have participated in the routing process have their value of residual energy reduced as compared to the other data sense points in the Sensing Field

NTTUA Method

Name	**Value**
Number of DSPs	100
Initial Level of Energy for SPs	3000 mJ
Number of Experimental Iterations	100
IDSP	42
DDSP	94
Coverage Area	40 m
Energy Required for data packet send	20 mJ
Energy Required for data packet generate	10 mJ
Attenuation factor	0.5

Table 28: Experimental Set Up NTTUA

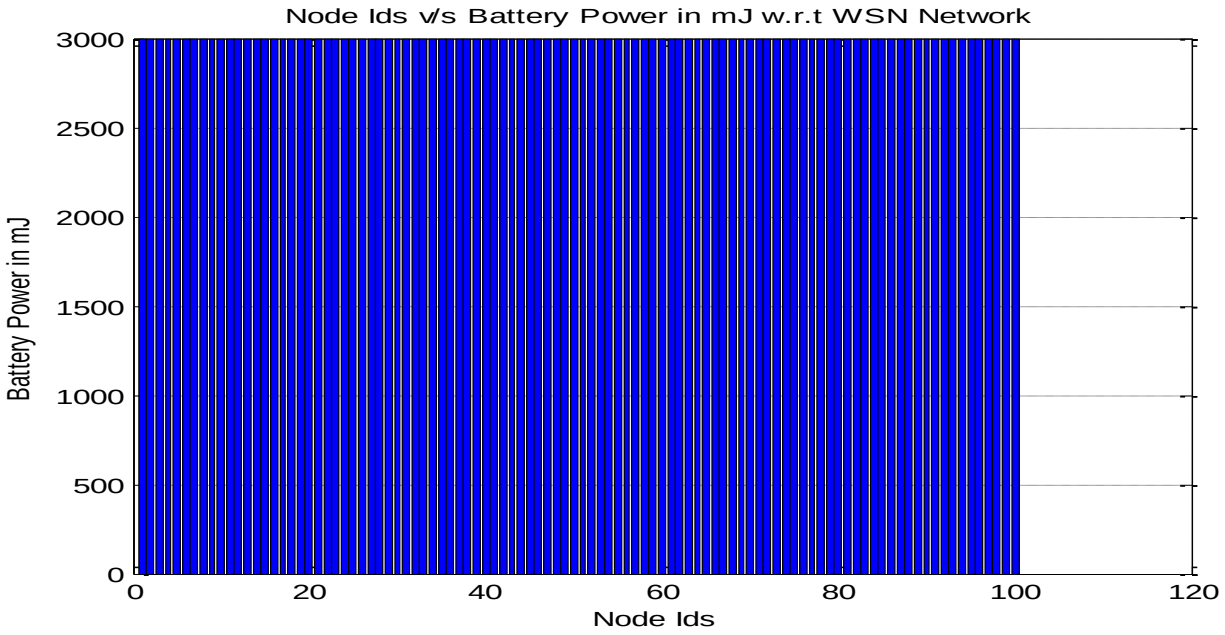

Fig 37: Battery Initialization for the Data sense points

Fig 37 shows the battery initialization for the data sense points in the Sensing Field. As shown in the fig all the 100 data sense points are initialized with the same amount of energy in the Sensing Field with a value of 3000 mJ.

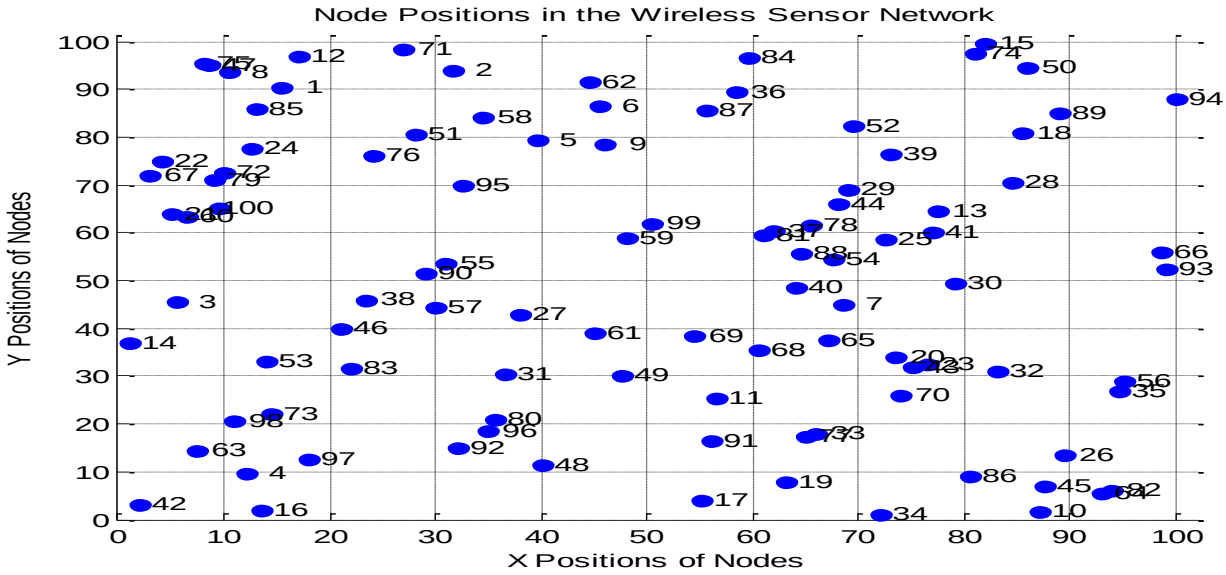

Fig 38: Data sense points Strategy Placement

Fig38 shows the data sense points strategic placement. As shown in the fig there are 100 data sense pointss in the Sensing Field and each data sense points will have its own unique position in the Sensing Field. Data sense points 42 is present at the location (2,4), Data sense points 10 will be placed at the location (88,2)

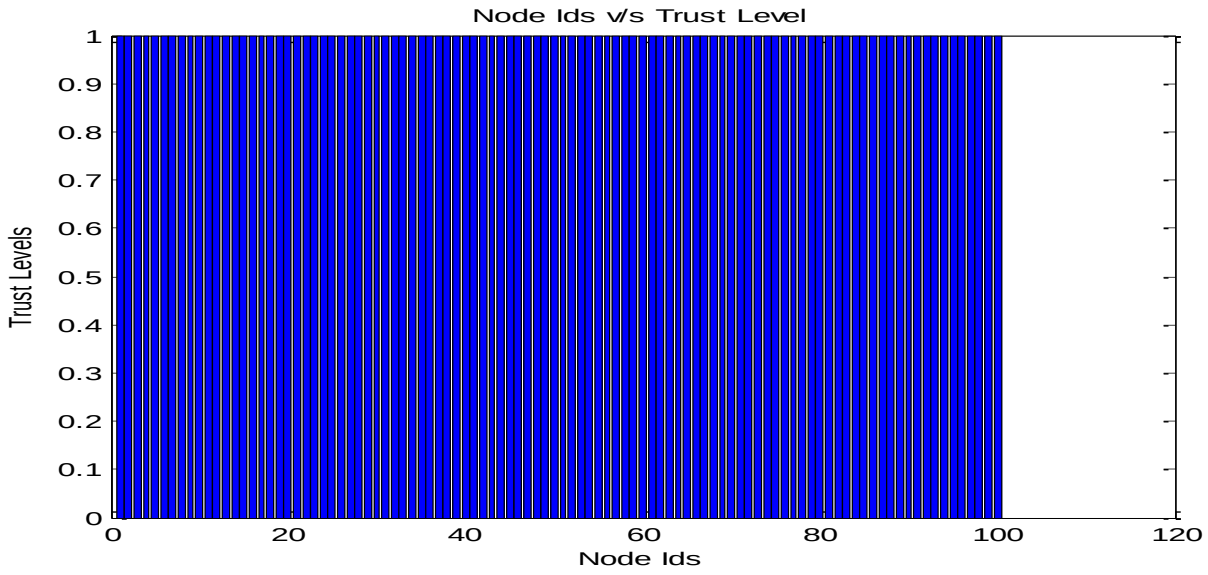

Fig 39: Trust Level Initialization

Fig39 shows the trust level initialization for all the data sense points in the Sensing Field. As shown in the fig all the 100 data sense points are initialized with the same value of trust i.e 1.

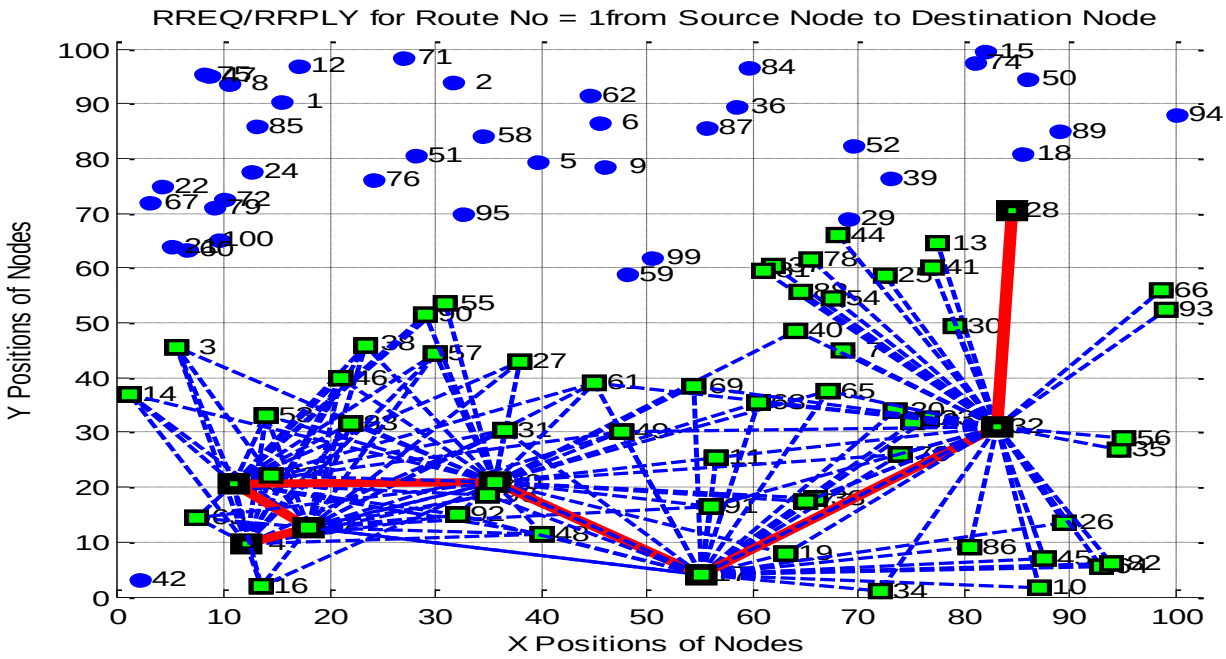

Fig 40: RREQ/RRLY for the Path1

Fig40 shows the RREQ/RRLY for the entire path1 in the Sensing Field. As shown in the fig there are blue lines which indicates the RREQ and the red lines indicates the REPLY to the initiating data sense points.

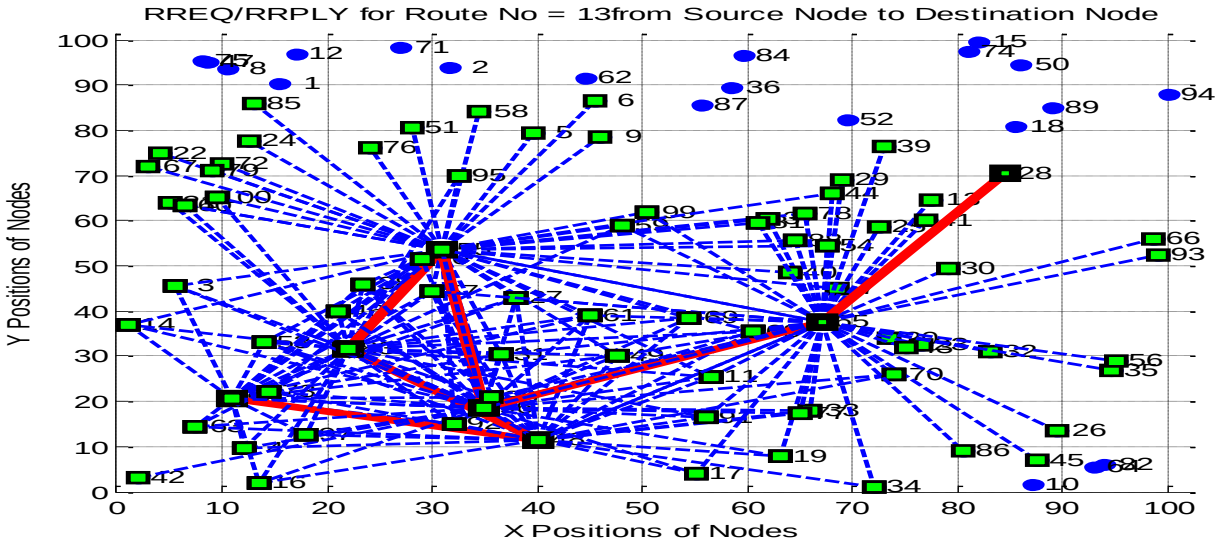

Fig 41: RREQ/RRLY for the Path13

Fig41 shows the RREQ/RRLY for the entire path13 in the Sensing Field. As shown in the fig there are blue lines which indicates the RREQ and the red lines indicates the REPLY to the initiating data sense points.

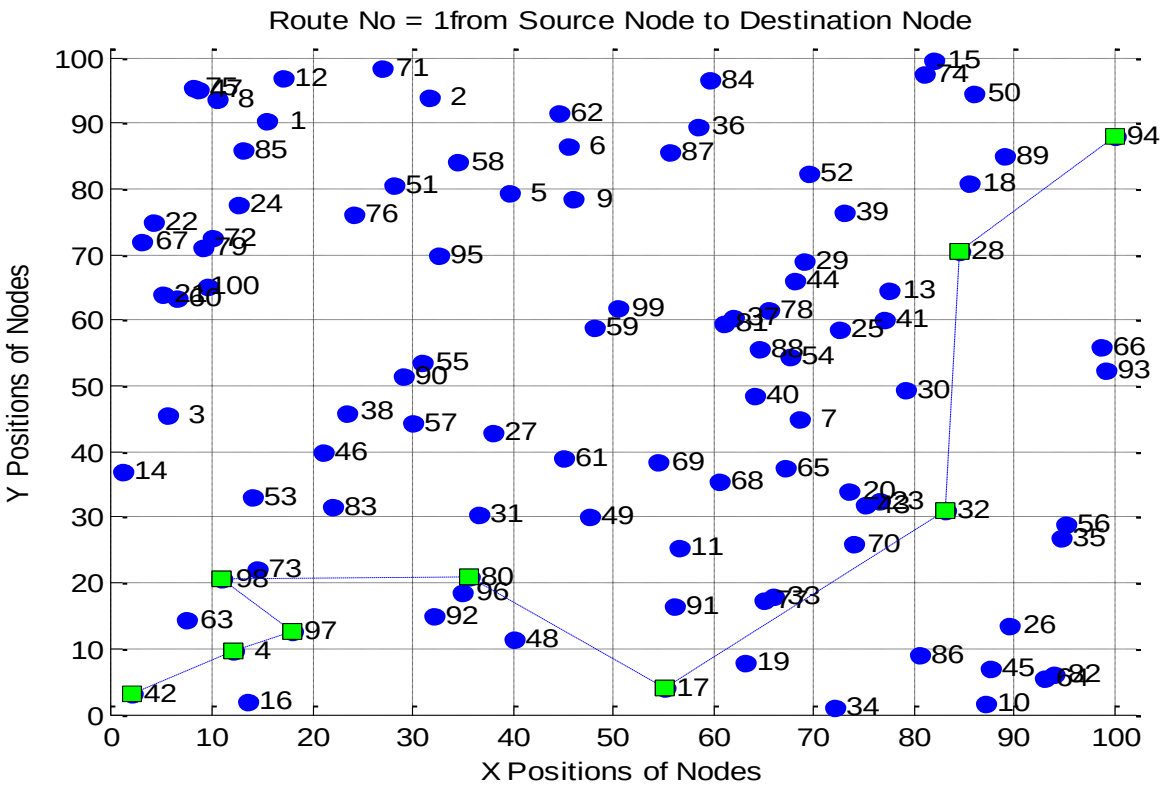

Fig42: Path1 between IDSP to DDSP

Fig 42 shows the complete path1 between initiator data sense points to destination data sense points and as shown in the fig the Data sense points 42 to Data sense points 94 the complete path1 is established.

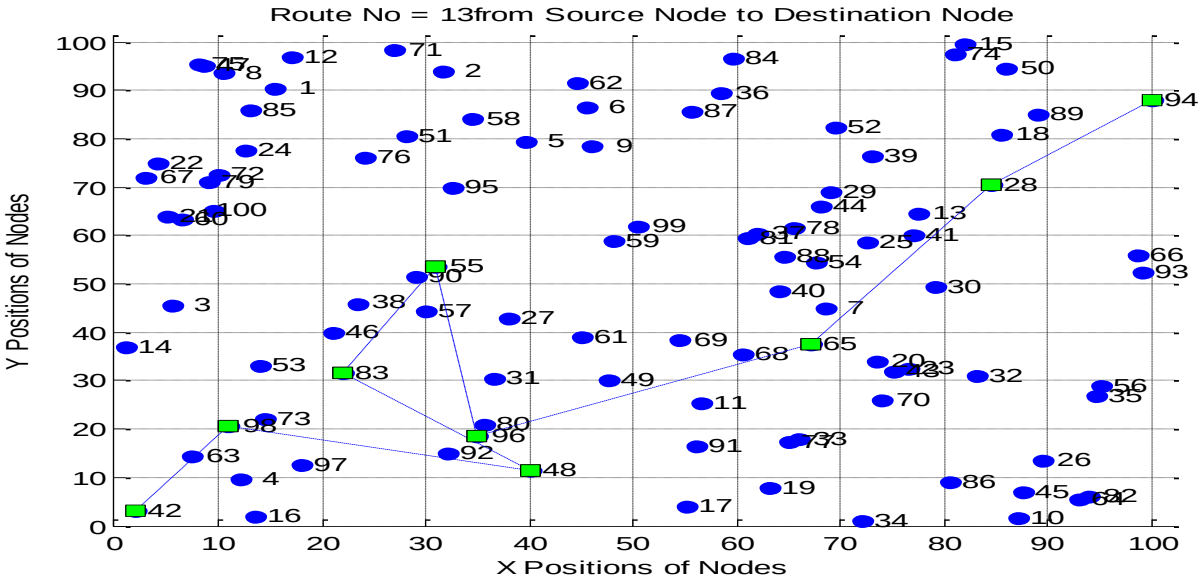

Fig 43: Path13 between initiator data sense points to destination data sense points

Fig43 shows the complete path13 between initiator data sense points to destination data sense points and as shown in the fig the Data sense points 42 to Data sense points 94 the complete path13 is established.

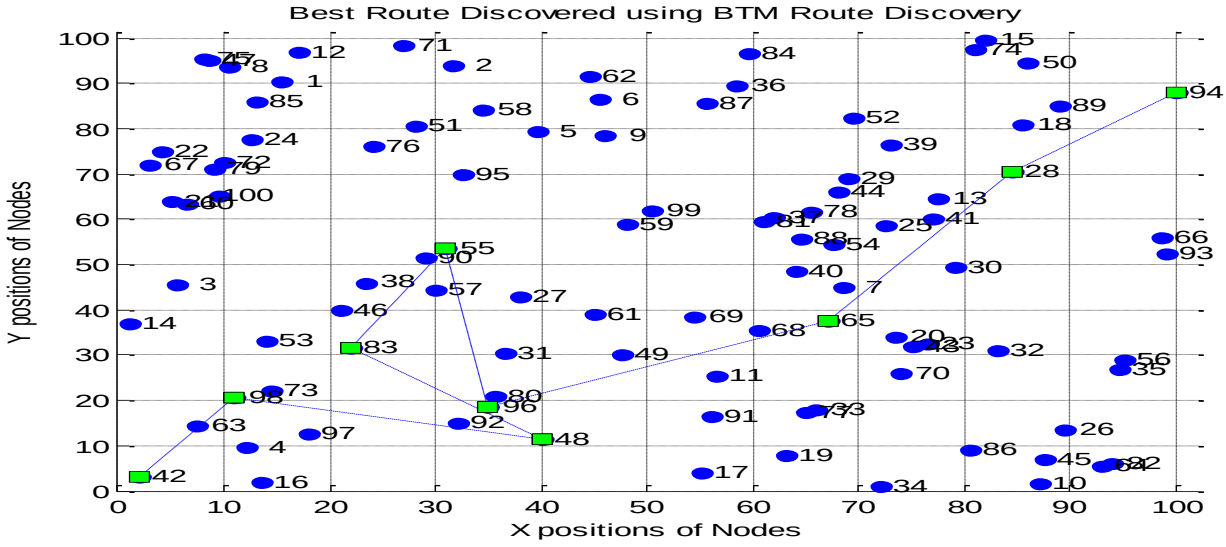

Fig44: Best Route Discovered between initiator data sense points to destination data sense points

Fig44 shows the complete best route discovered between initiator data sense points to destination data sense points and as shown in the fig the Data sense points 42 to Data sense points 94 the complete path13 is established.

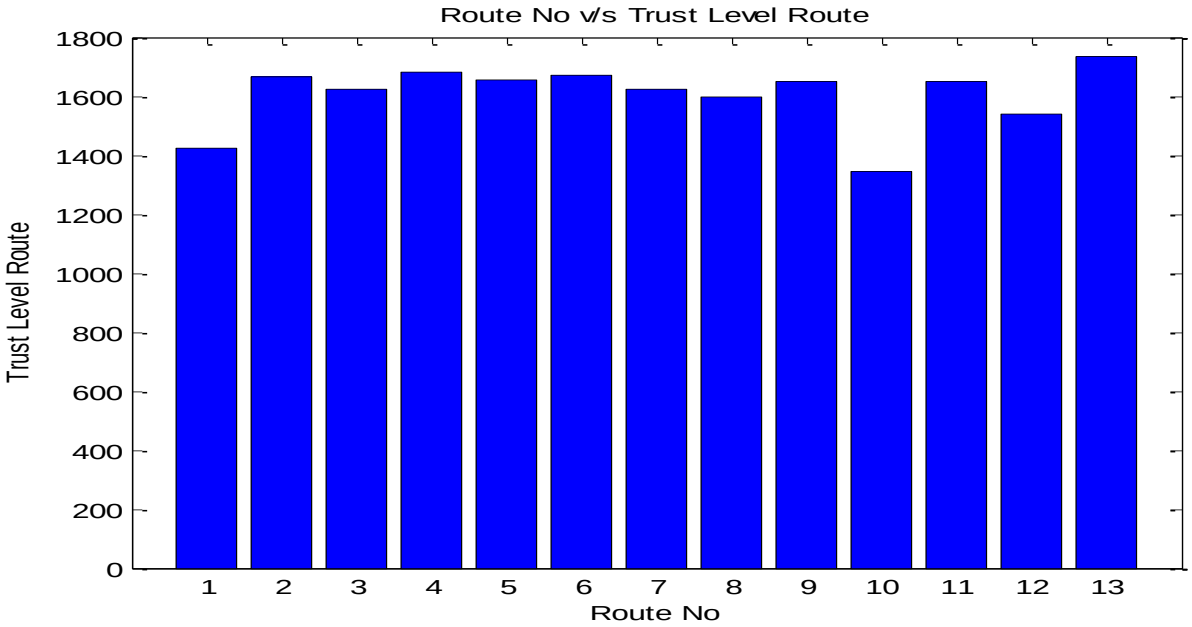

Fig 45: Route No versus Trust Level

Fig 45 shows the route number versus trust level for all the routes in the Sensing Field. The route number 13 is having the highest trust level.

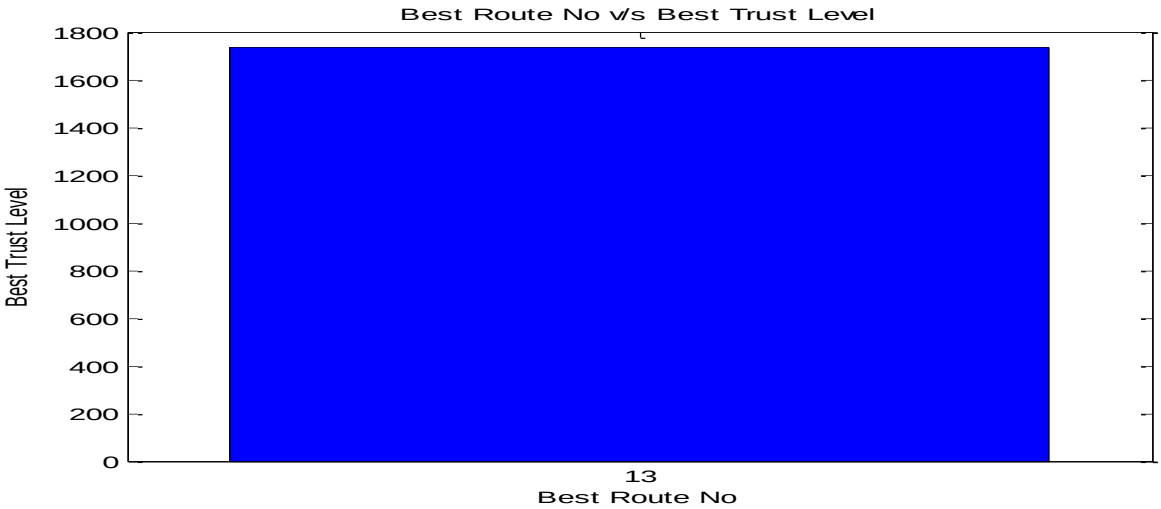

Fig 46: Best Route Number v/s Trust Level

Fig46 shows the best route number v/s trust level. As shown in the fig route 13 is the best route and is having the highest trust level in the Sensing Field.

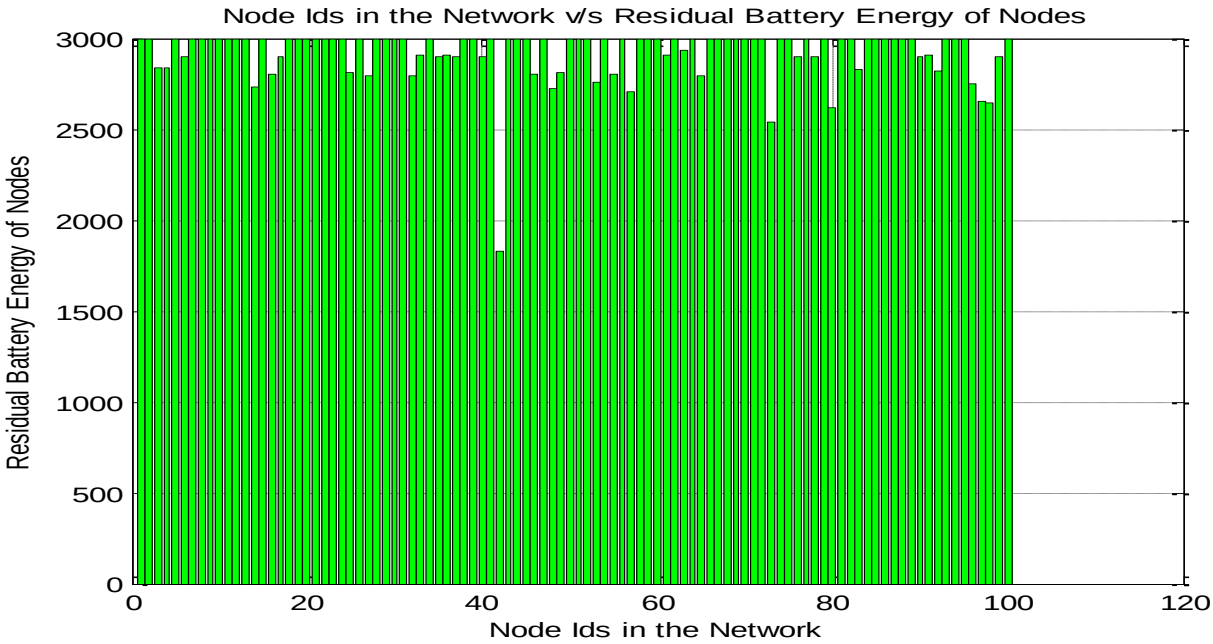

Fig47: Remaining Battery Levels for the Data sense points

Fig47 shows the remaining battery level for the data sense points in the Sensing Field. As shown in the Sensing Field the data sense points which participate in routing will have lesser battery when they participate in the path

COMPARISION RESULTS

This section compares the proposed method with that of previous method

Name	**Value**
Number of DSPs	100
Initial Level of Energy for SPs	3000 mJ
Number of Experimental Iterations	100
IDSP	42
DDSP	94
Coverage Area	40 m
Energy Required for data packet send	20 mJ
Energy Required for data packet generate	10 mJ
Attenuation factor	0.5
Number of Iterations	100

Table 29: Experimental Set Up NTTUA

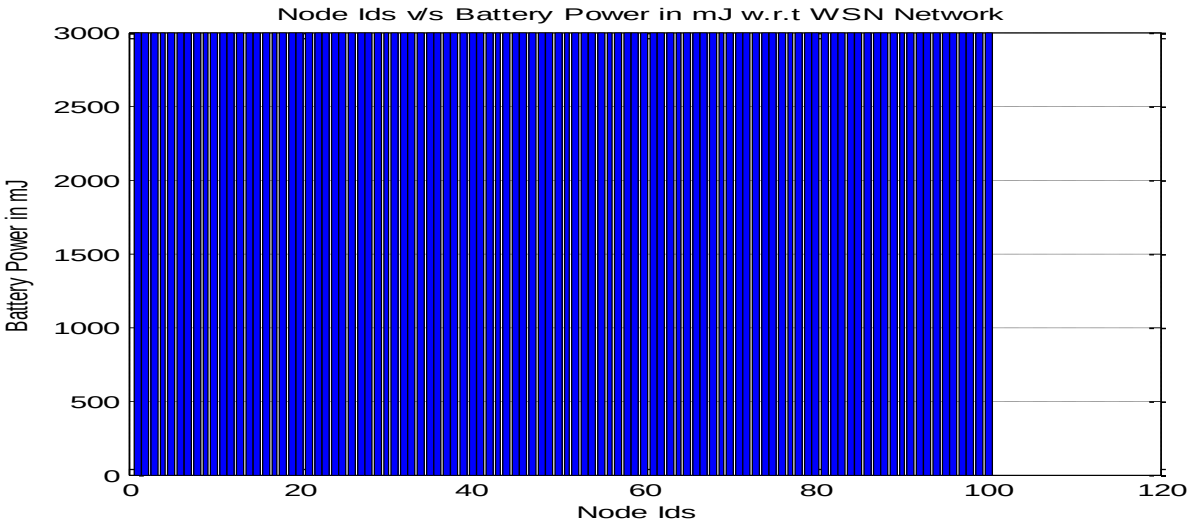

Fig 48: Battery Initialization for the Sensing Field

Fig 48 shows the battery initialization for all the 100 data sense points in the Sensing Field. As shown in the fig all the 100 data sense points are initialized with the same amount of energy of about 3000 mJ.

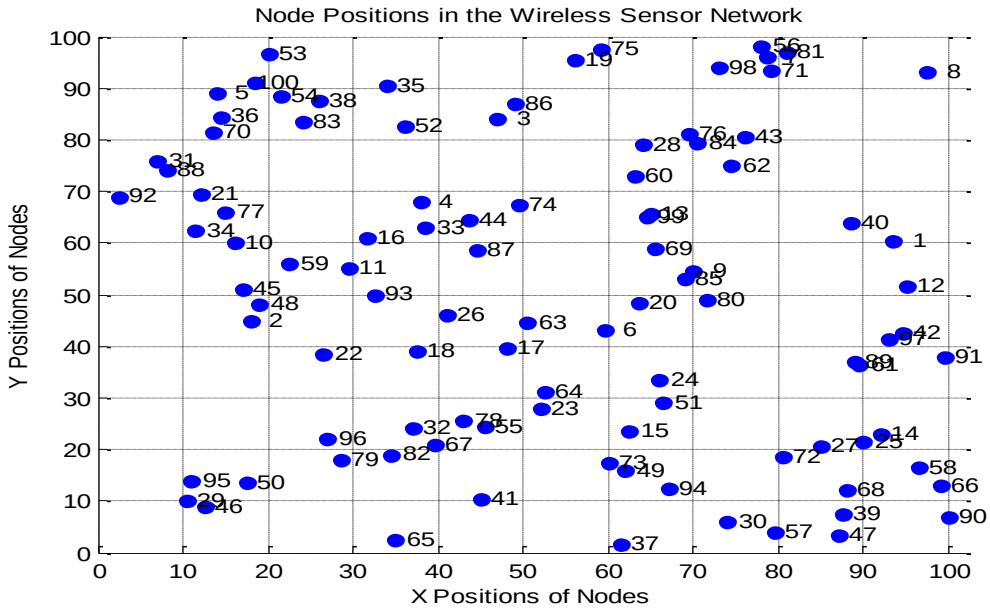

Fig49: Data sense points Placement Strategy

Fig 49 shows the data sense points placement strategy as shown in the fig there 100 data sense points spread across the area of 100*100 meters. Data sense points 65 is at the location of (35,2), Data sense points 57 is at the location (80,2), in a similar fashion each of the remaining 98 data sense points have their own unique positions in the Sensing Field.

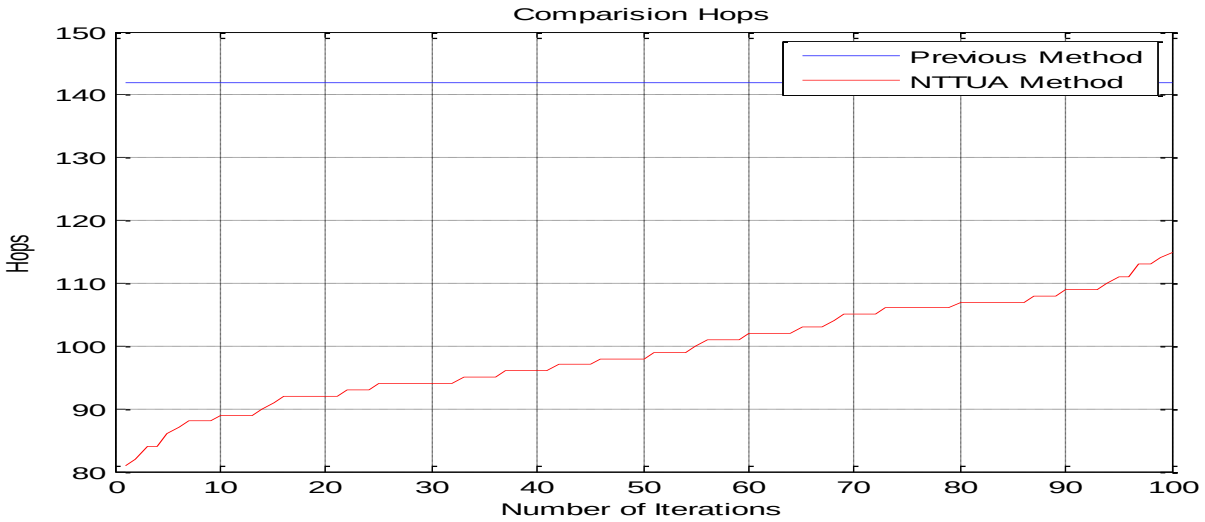

Fig 50: Comparison of Hops

Fig50 shows the comparison of hops with respect to previous method and the proposed NTTUA method. As shown in the fig as the number of iterations increases the hops of NTTUA method will increase whereas the Previous Bayesian method has constant and high number of hops. The proposed method has lower hops and the hops are within the range of 80 to maximum 118 hops as compared to previous method which is always higher than 140 hops. The hops are not for the best path but for all possible paths in the proposed and previous approach.

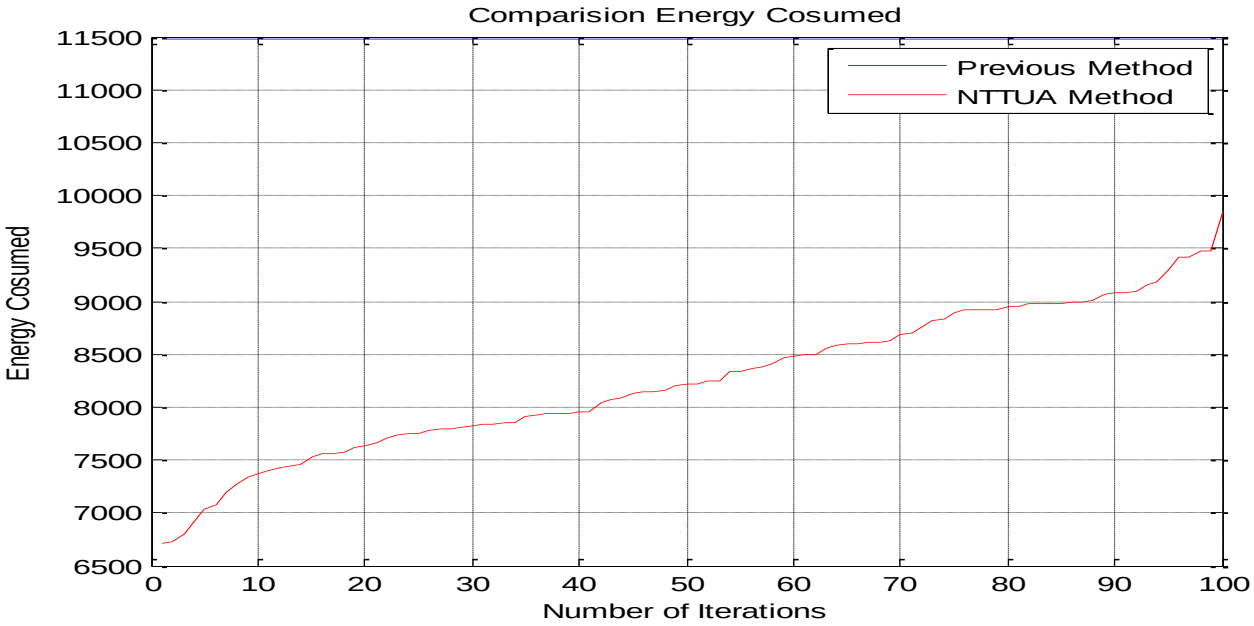

Fig 51: Energy Consumption Comparison

Fig shows the energy consumption comparison between the previous method and the proposed method. As shown in the fig as the number of iterations increases the energy consumption also increases with the number of iterations. The Proposed method has lower energy consumption as compared to previous method. The maximum value of energy consumed for proposed is around 9700 mJ but for the previous method it is always higher across all iterations and is well above 11000 mJ

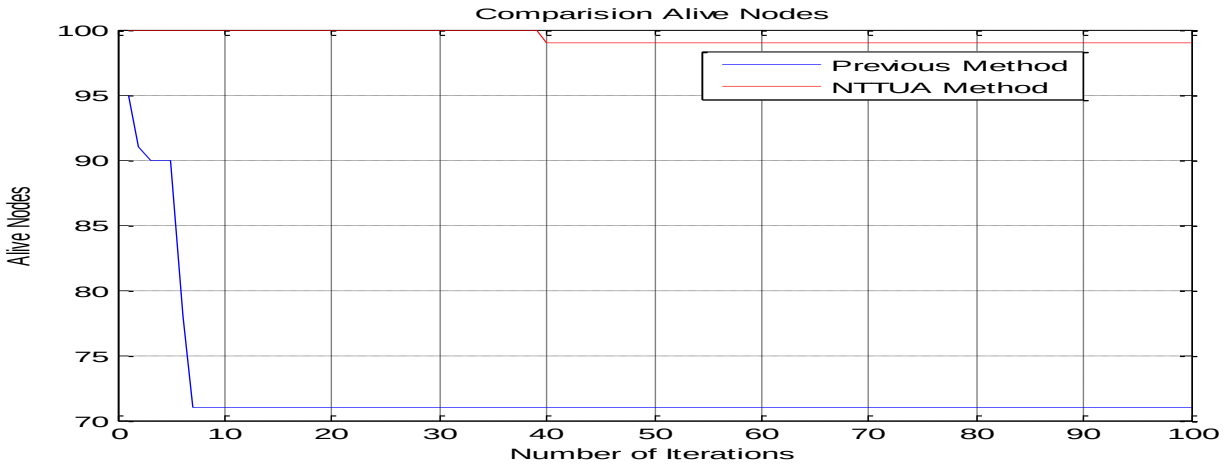

Fig 52: Number of Efficient Data sense points

Fig 52 shows the number of Efficient data sense points. As shown in the fig the proposed method has more number of Efficient data sense points as compared to previous method. Also, as the number of iterations increases the number of Efficient data sense points are coming down. At the end of 100 iterations there are 99 Efficient data sense points for the proposed where as for the previous method the number of Efficient data sense points are around 72.

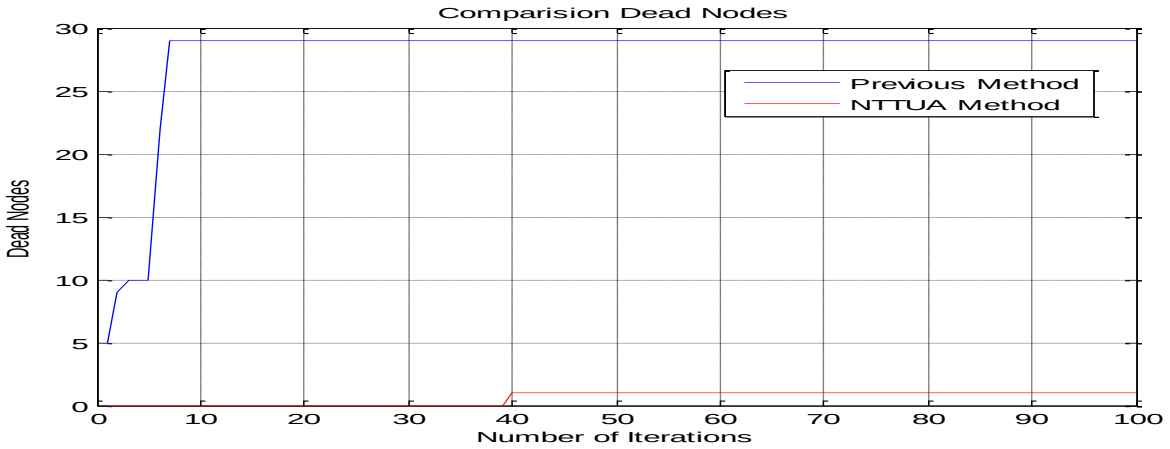

Fig53: Number of Dead Data sense points

Fig 53 shows the comparison of number of dead data sense points between the previous method and NTTUA method. As shown in the fig the number of dead data sense points are higher for the previous method and they are increasing as the number of iterations increases. At the end of 100 iterations there are 28 dead data sense points for the previous method but for NTTUA method the number of such dead data sense points are around 2.

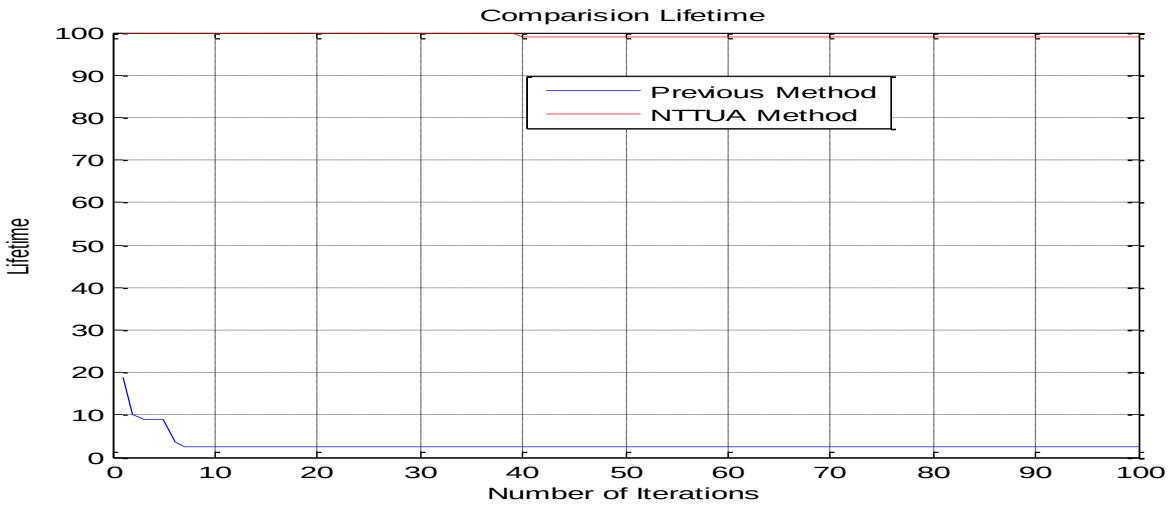

Fig 54: Lifetime Ratio

Fig 54 shows the comparison of lifetime ratio between the proposed NTTUA method along with the previous method. As shown in the fig the proposed method has the higher lifetime as compared to previous method. The lifetime for the proposed method has the highest value of 100% and at the end of 100 iterations it is 99% the previous method lifetime has highest 19% and lowest 1%

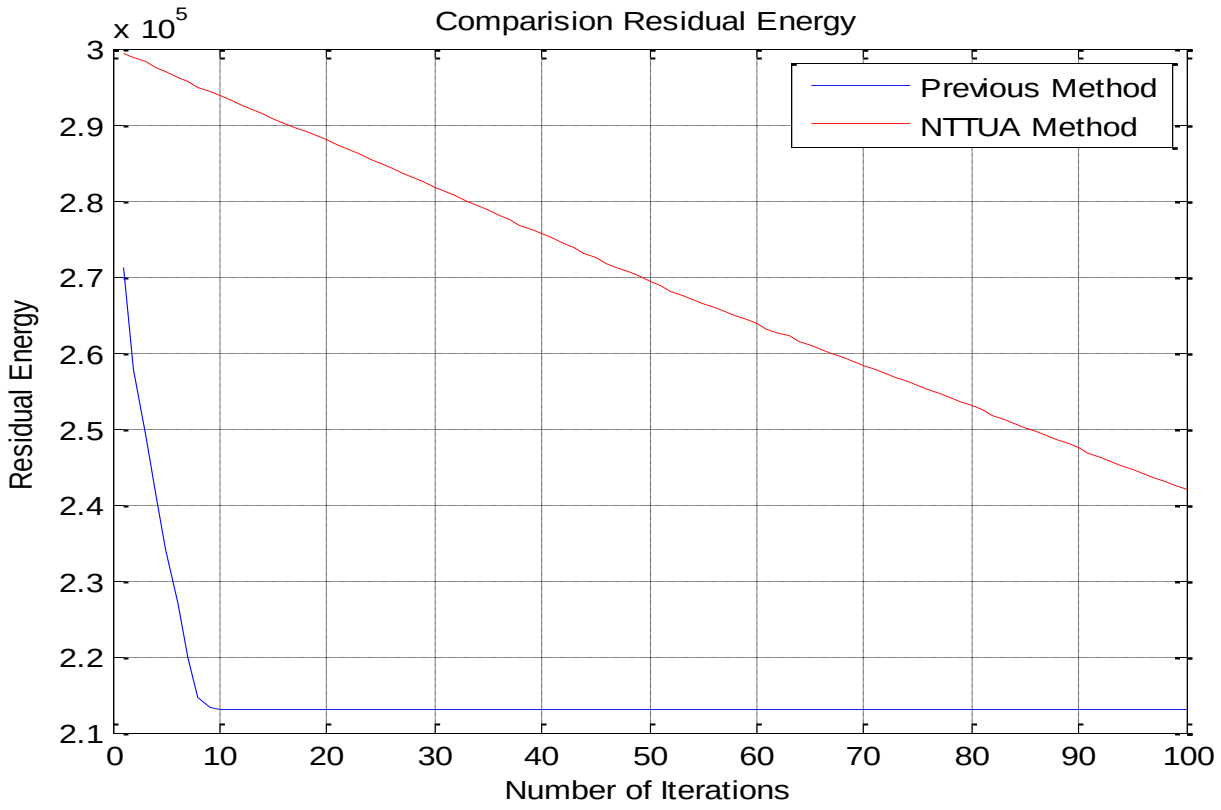

Fig 55: Residual Energy Comparison

Fig55 shows the residual energy comparison between the two algorithms namely Previous Method and NTTUA method. As shown in the fig the proposed NTTUA method has higher residual energy as compared to previous method. Also, as the number of iterations increases the residual energy for the methods also decreases. At the end of 100 iterations the amount of residual energy for the proposed NTTUA method is around 2.4* 10^ 5 as compared to previous method which is about 2.1*10^5. Hence proposed method is behaving well for the case of residual energy

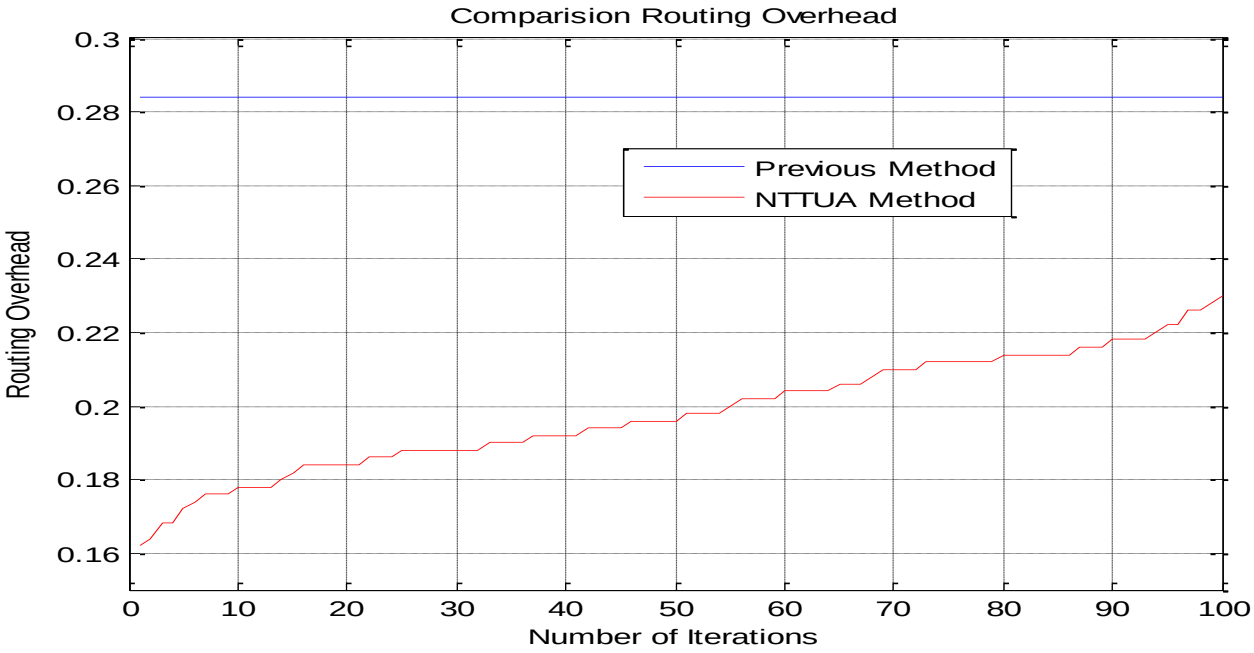

Fig 56: Overhead Comparison

Fig56 shows the overhead comparison between the previous method and NTTUA method. As shown in the fig overhead of the proposed method is lesser as compared to the previous method. Also, as the number of iterations increases the overhead ratio is also increasing. The overhead of the previous method always is above 0.28 but for the proposed method lowest is 0.17 and highest is around 0.23 hence with respect to overhead proposed method is behaving well.

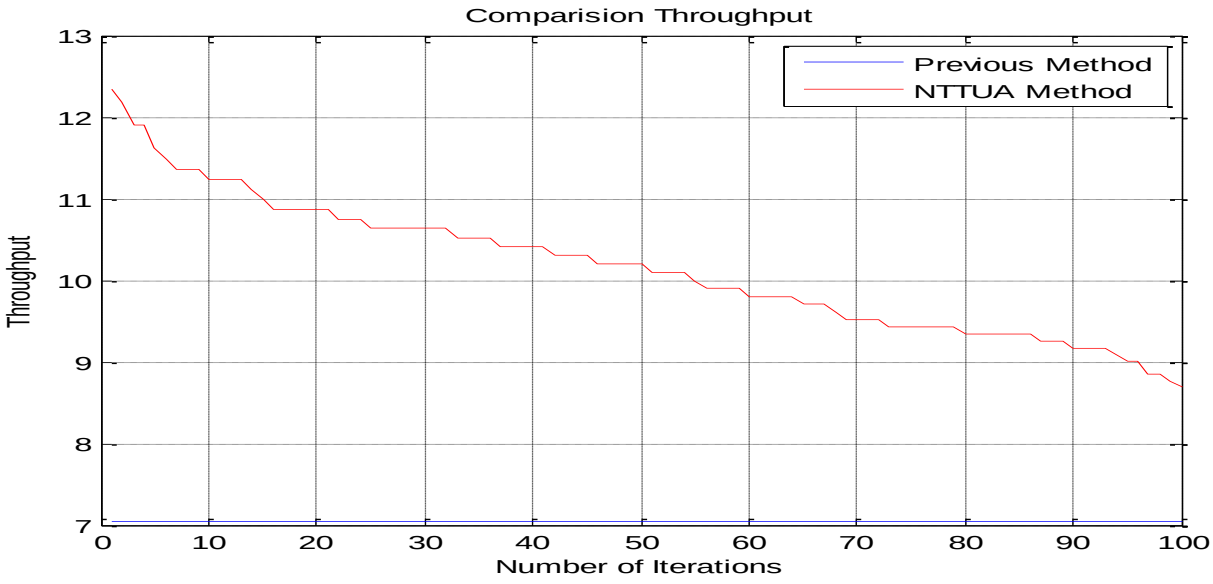

Fig 57: Throughput

Fig 57 shows the throughput comparison between the proposed and previous method. As shown in the fig as the number of iterations increases the throughput will come down drastically. The proposed NTTUA method has higher throughput as compared to previous method across all the 100 iterations.

The overall comparison between the two methods for the set of 100 iterations can be defined as follows

Parameter	Improvement with respect to Bayesian Method in Percentage
Time	22.10 %
Links Hops	36.39%
Energy Utilization	37.09%
Lifetime Ratio	17.02%
Throughput	36.39%
Residual Energy	36.43%

Table 30: *Percentage Improvement for 100 iterations with 100 nodes*

Table 30 shows the percentage improvement of the proposed method NTTUA improvement with respect to existing Bayesian method. The number of nodes taken into consideration on a 100*100 area were 100 nodes. With random positions occupied by each of the nodes. All nodes were initialized by 500 J of battery energy. The energy required for transmission was set to 20 J, Energy for amplification was set to 10J along with attenuation factor of 0.5. From the table one can observe that the proposed method has overall improvement of 22.10% as compared to previous with respect to time. The percentage improvement is 36.39% with respect to hops, energy utilization is reduced by a factor of 37.09% as compared to Bayesian method. The lifetime ratio has been improved by a factor of 17.02% along with throughput with an improvement of 36.39% and finally residual energy is improved by 36.43%.

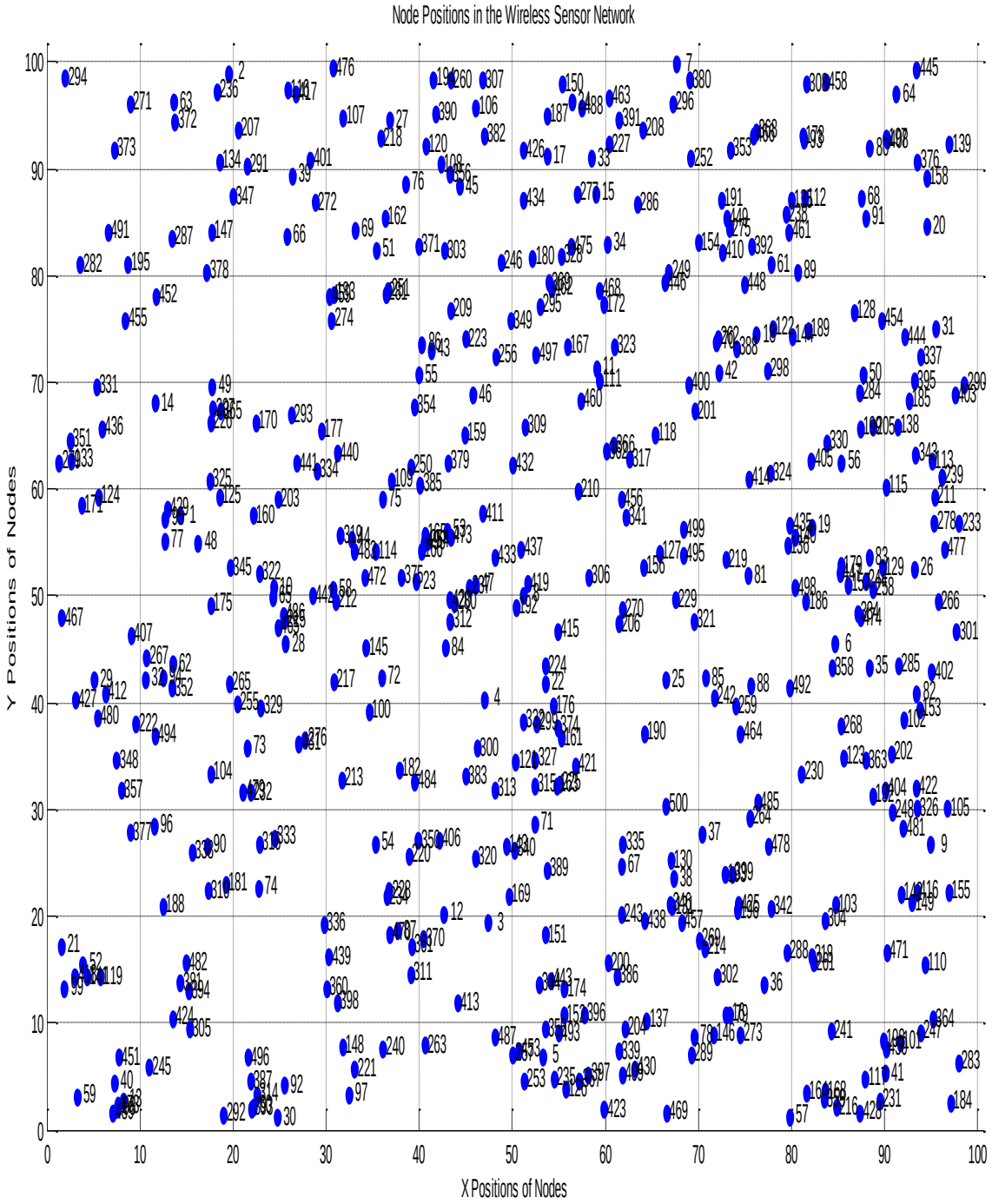

Fig 58: Node Deployment Algorithm

Fig shows the node deployment algorithm. As shown in the fig there are 500 nodes spread across 100 *100 area. The communication is formed is from Node 59 to Node 64.

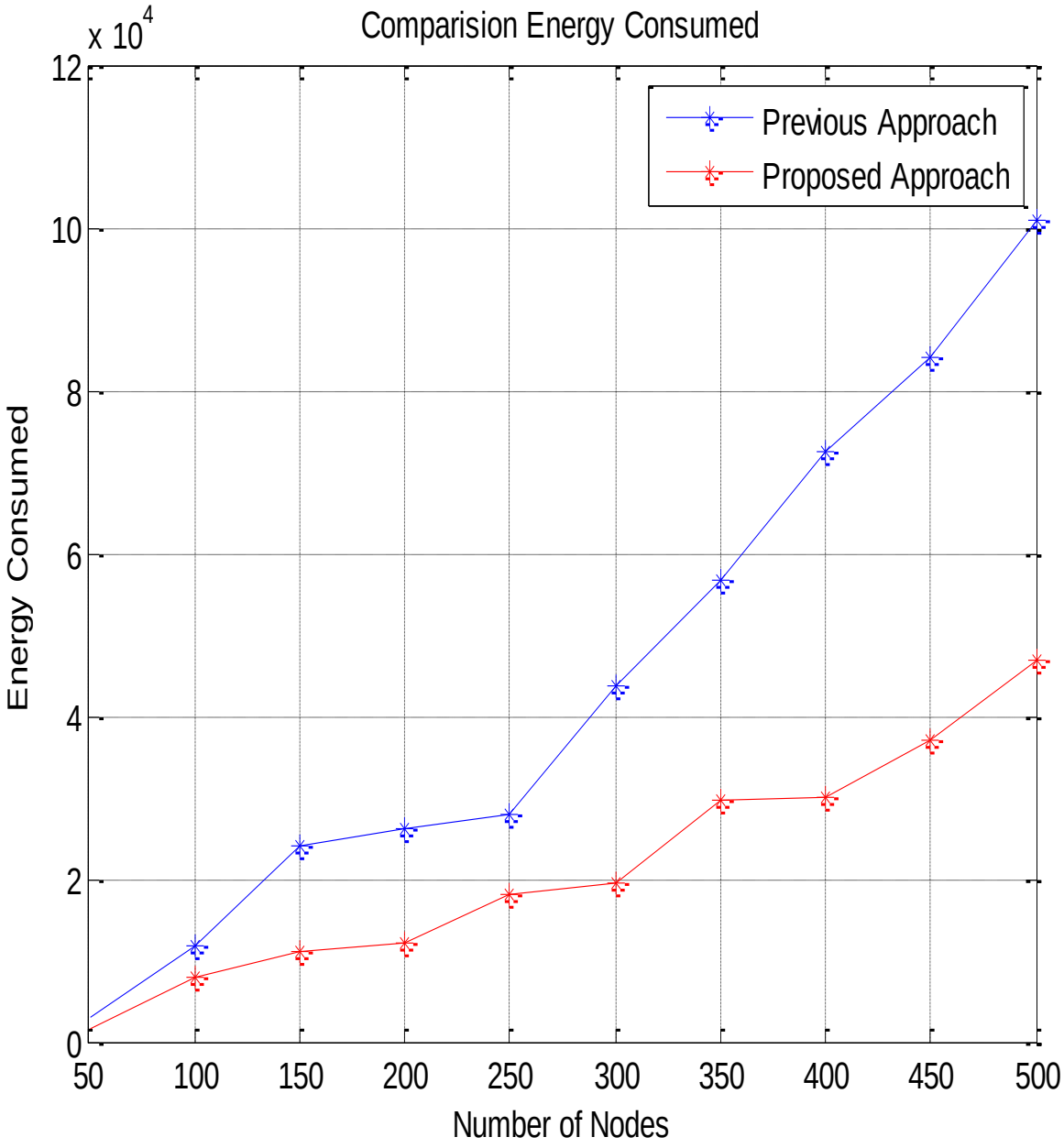

Fig59: Energy Consumed Comparison

Fig shows the energy consumed comparison. As shown in the fig the energy consumption increases as the number of nodes increases for both proposed and previous methods. For the set of nodes with the values starting from 50 nodes to 500 nodes. The energy consumption

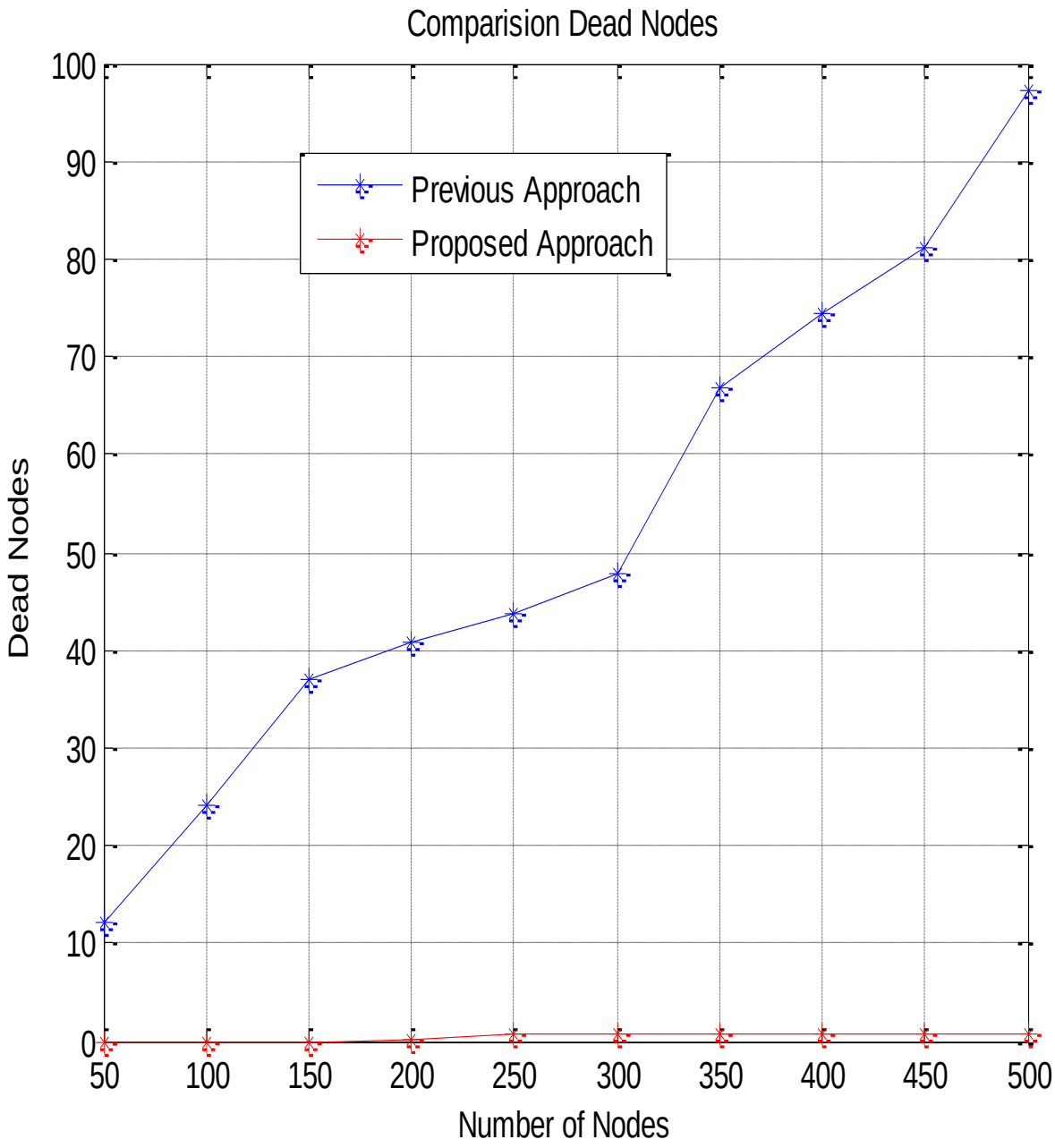

Fig60: Comparison Dead Nodes

Fig shows the comparison dead nodes. As shown in the fig the number of dead nodes are increasing as the number of nodes increases. For the 50 nodes there are 0 dead nodes for the proposed method whereas 11 nodes which are dead in the previous approach. In a similar fashion as the number of nodes in network increases the dead nodes also increases but at the end with 500 nodes comparison 98 nodes are dead for previous approach but only 2 nodes are dead for the case of proposed approach.

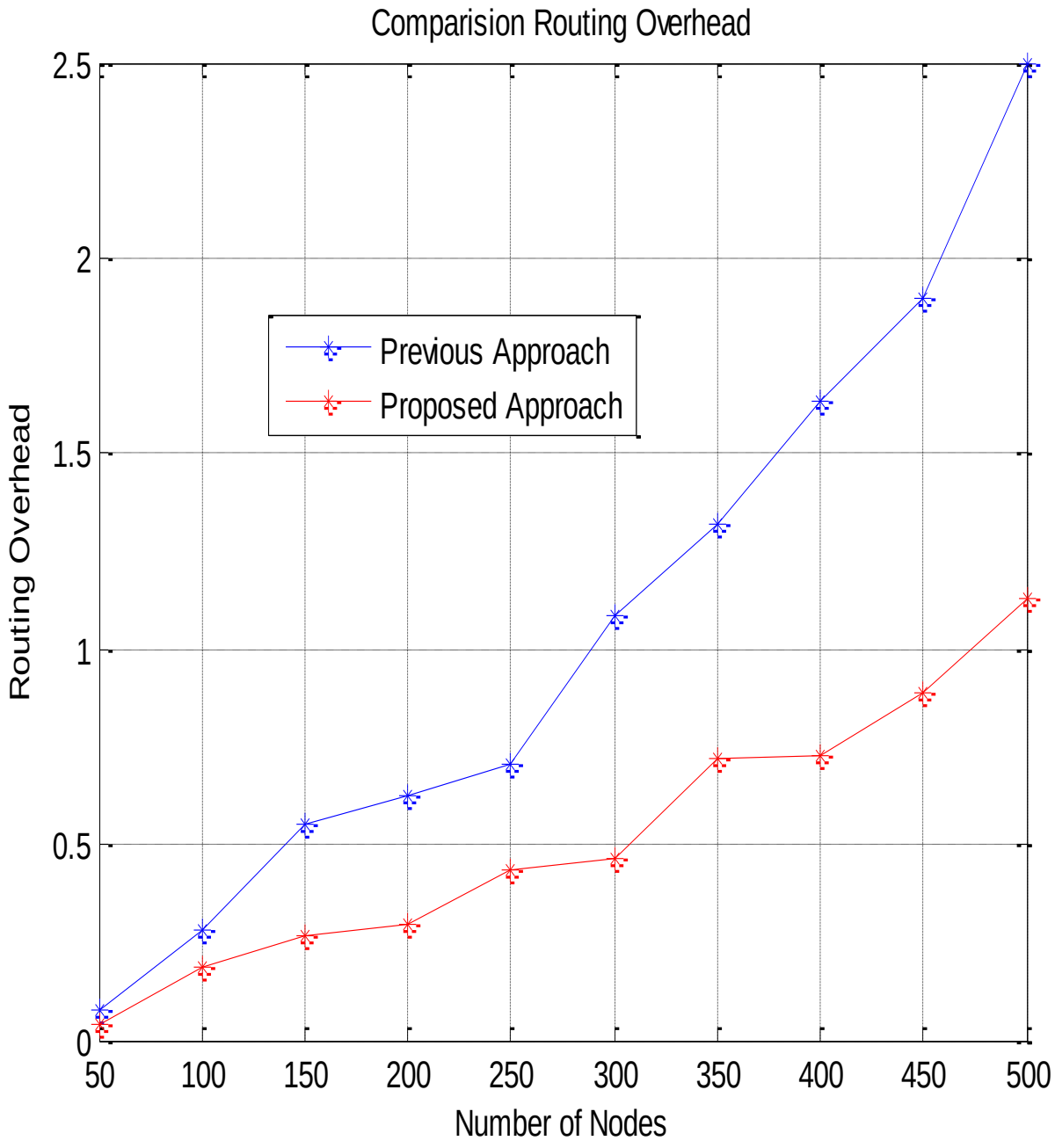

Fig61: Routing Overhead

Fig shows the routing overhead comparison from the 50 nodes to 500 nodes. As the number of iterations increases the routing overhead increases. The routing overhead for the 50 nodes is less than 0.1 as compared to previous approach which has 0.12 as the routing overhead. At the end 500 nodes will have routing overhead of 1.2 as compared to a value of 2.5.

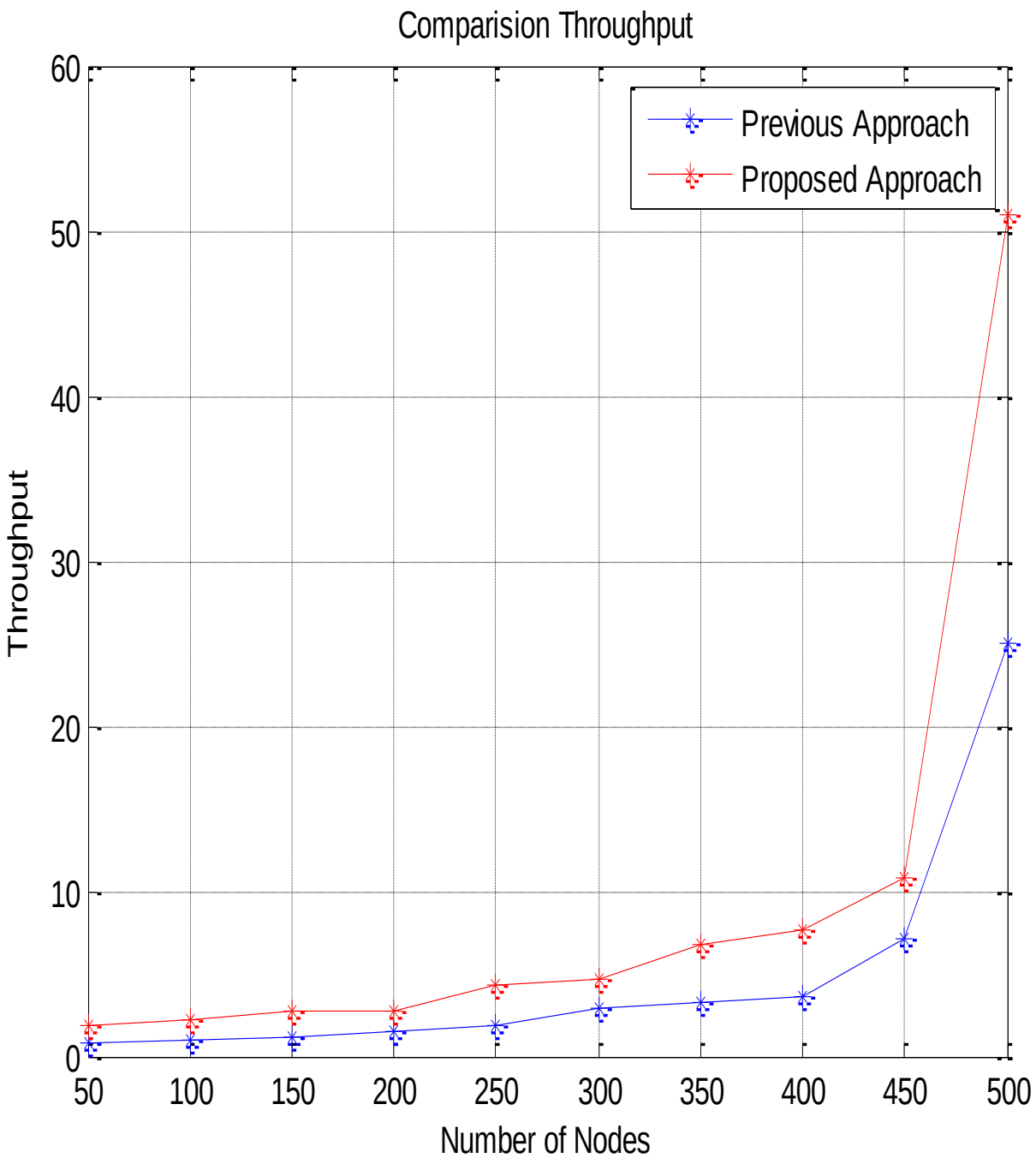

Fig62: Throughput Comparison

Fig shows the throughput comparison between the proposed and previous method. As shown in the fig the number of nodes are increased from 50 to 500. The throughput is increasing this is because of the number of nodes sensing the area are increasing. The throughput of the proposed method is always higher as compared to previous method.

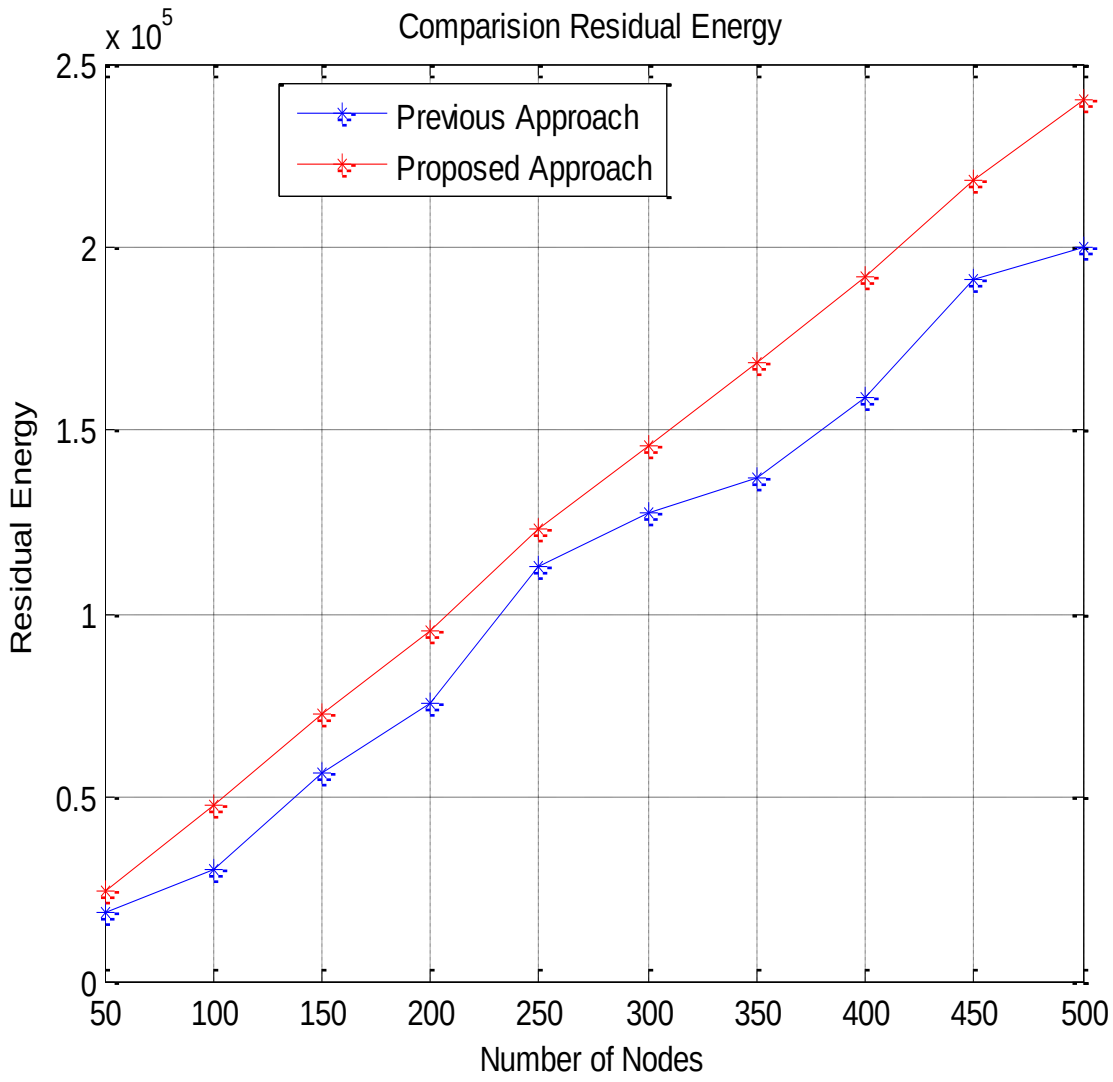

Fig 63 Residual Energy Comparison

Fig 63 shows the residual energy comparison by increasing the number of nodes from 50 to 500. Since the residual energy is the sum of remaining energy of all the nodes in the network it increases as the number of nodes in the network increases. For every 50, 100, 150 till 500 nodes the residual energy of proposed method is always higher as compared to the proposed method.

CHAPTER 8
CONCLUSION AND FUTURE SCOPE

8.1 CONCLUSION

In this project first the definition of data sense points, different kind of data sense points regions and the Sensing Field chosen for the project implementation is described. The previous approach based on direct trust measure which depends upon only the packet acknowledgement is described and then followed by the proposed method which makes use of direct trust along with that the method will also make use of Sensing Field security index, packet loss measure in order to compute the trust and then the data sense points which has the highest trust is taken as the next forward data sense points. The previous approach is also compared with proposed method with respect to delay, hops, energy consumed, number of alive data sense points, number of dead data sense points, lifetime ratio, residual energy, overhead ratio, throughput.

8.2 FUTURE SCOPE

[1] The project can be future improved by making use of Data sense points Recovery algorithm in order to recover dead data sense points in the Sensing Field by making use of genetic algorithm.

[2] The improvisation can also be done by placing relay data sense points at regular intervals which can help in reducing the overall hops for the end to end path formation.

[3] The project can be future improved by implementing the algorithm on the real sensor devices[cisco] and comparing it with the simulation results

8.3 CONTRIBUTION

The contribution to the project on top of existing NTTUA is that additional parameters like residual energy, efficient, non-efficient nodes, lifetime ratio and throughput are also computed. Also, during the forward node pick the residual energy is computed for all the DSPs within the transmission range so that overall lifetime and throughput is improved apart from trust level computation

CHAPTER 9

BIBLIOGRAPHY

[1]V. Potdar, A. Sharif, and E. Chang, "*Wireless sensor networks: A survey," in Advanced Information Networking and Applications* Workshops, International Conference on 2009, pp. 636-641.

[2] V. Gungor and G. Hancke, "*Industrial wireless sensor networks: Challenges, design principles, and technical approaches*," IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4258–4265,October 2009.

[3] "*Wireless sensor networks: A survey*," Computer Networks,vol. 38, no. 4, pp. 393–422, March 2002.

[4] K. Romer and F. Mattern, "*The design space of wireless sensor networks*," IEEE Wireless Communications, vol. 11, no. 6, pp. 54–61,December 2004.

[5] D. Puccinelli and M. Haenggi, "*Wireless sensor networks: Applications and challenges of ubiquitous sensing*," IEEE Circuits and Systems Magazine, vol. 5, no. 3, pp. 19–31, September 2005.

[6] Jan Bauer,Nils Aschenbruck,"*Design and implementation of an agricultural monitoring system for smart farming*", 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany),8-9 May 2018

[7] Elisa Pievanelli ; Alina Plesca ; Riccardo Stefanelli ; Daniele Trinchero,"Dynamic wireless sensor networks for real time safeguard of workers exposed to physical agents in constructions sites",2013 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet),20-23 Jan. 2013

[8] M. Udin Harun Al Rasyid ; Doni Prasetyo ; Isbat Uzzin Nadhori ; Ali Husein Alasiry,"*Mobile monitoring of muscular strain sensor based on Wireless Body Area Network*",2015 International Electronics Symposium (IES),29-30 Sept. 2015

[9] Abel Rodriguez de la Concepcion ; Riccardo Stefanelli ; Daniele Trinchero,"*Adaptive wireless sensor networks for high-definition monitoring in sustainable agriculture*",2014 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet),19-23 Jan. 2014

[10] M. Benaddy ; B. El Habil ; M. El Ouali ; O. El Meslouhi ; S. Krit,"*A mutlipath routing algorithm for wireless sensor networks under distance and energy consumption constraints for reliable data transmission*",2017 International Conference on Engineering & MIS (ICEMIS), 8-10 May 2017

[11] Navdeep Singh Randhawa ; Mandeep Dhami,"*Reduction of Energy Consumption in WSN using Hybrid VGDRA Approach*",2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS),10-12 Oct. 2018

[12] Mohammed Abo-Zahhad ; Mohammed Farrag ; Abdelhay Ali ; Osama Amin,"*An energy consumption model for wireless sensor networks*", 5th International Conference on Energy Aware Computing Systems & Applications,24-26 March 2015

[13] Er. Robin Chadha ; Love Kumar ; Er. Jatinderpal Singh,"3 Dimensional WSN: An energy efficient network",2017 2nd International Conference for Convergence in Technology (I2CT),7-9 April 2017

[14] Nishakumari Lodha ; Prasant Rewagad ; Yogita Pawar,"Simulation of MTMS Using TSSE and Minimum Energy Consumption Using DVS for WSN Ad Hoc Network",
2014 Fourth International Conference on Communication Systems and Network Technologies,7-9 April 2014

[15] Mohammed Abo-Zahhad ; Mohammed Farrag ; Abdelhay Ali,"Modeling and minimization of energy consumption in wireless sensor networks", 2015 IEEE International Conference on Electronics, Circuits, and Systems (ICECS),6-9 Dec. 2015

[16] Abhishek Chunawale ; Sumedha Sirsikar,"Minimization of average energy consumption to prolong lifetime of Wireless Sensor Network", 2014 IEEE Global Conference on Wireless Computing & Networking (GCWCN),22-24 Dec. 2014

[17] Najmeh Kamyabpour ; Doan B. Hoang,"Statistical Analysis to Extract Effective Parameters on Overall Energy Consumption of Wireless Sensor Network (WSN)",2012 13th International Conference on Parallel and Distributed Computing, Applications and Technologies,14-16 Dec. 2012

[18] Pramod D. Ganjewar ; Sanjeev. J. Wagh ; Barani S.,"Threshold based data reduction technique (TBDRT) for minimization of energy consumption in WSN", 2015 International Conference on Energy Systems and Applications,30 Oct.-1 Nov. 2015

[19] Dietrich and F. Dressler, "*On the lifetime of wireless sensor networks*,"ACM Transactions on Sensor Networks, vol. 5, no. 1, pp. 1–39,February 2009.

[20] M. Najimi, A. Ebrahimzadeh, S. Andargoli, and A. Fallahi, "*Lifetime maximization in cognitive sensor networks based on the sensing point selection*," IEEE Sensors Journal, vol. 14, no. 7, pp. 2376–2383, July 2014.

[21] Y. Chen and Q. Zhao, "*On the lifetime of wireless sensor networks*," IEEE Communications Letters, vol. 9, no. 11, pp. 976–978, November 2005.

[22] J. W. Jung and M. Weitnauer, "*On using cooperative routing for lifetime optimization of multi-hop wireless sensor networks: Analysis and guidelines*," IEEE Transactions on Communications, vol. 61, no. 8,pp. 3413–3423, August 2013.

[23] C. Cassandras, T. Wang, and S. Pourazarm, "*Optimal routing and energy allocation for lifetime maximization of wireless sensor networks with nonideal batteries*," IEEE Transactions on Control of Network Systems, vol. 1, no. 1, pp. 86–98, March 2014.

[24] B. Bejar Haro, S. Zazo, and D. Palomar, "*Energy efficient collaborative beamforming in wireless sensor networks*," IEEE Transactions on Signal Processing, vol. 62, no. 2, pp. 496–510, January 2014

[25] M. Bhardwaj and A. P. Chandrakasan, "*Bounding the lifetime of sensor networks via optimal role assignments*," in IEEE International Conference on Computer Communications (INFOCOM'02), vol. 3, NY,USA, June 2002, pp. 1587–1596.

[26] S. Soro and W. Heinzelman, "*Prolonging the lifetime of wireless sensor networks via unequal clustering*," in IEEE International Parallel and Distributed Processing Symposium, Denver, CO, April 2005.

[27] B. C˘arbunar, A. Grama, J. Vitek, and O. C˘arbunar, "*Redundancy and coverage detection in sensor networks*," ACM Transactions on Sensor Networks (TOSN), vol. 2, no. 1, pp. 94–128, February 2006.

[28] R. Llanos, S. Martinez, "Distributed and robust fair optimization applied to virus diffusion control," IEEE Transactions on Sensing Field Science and Engineering, vol. 4, no. 1, pp. 41–54, 2017.

[29] S. Shirali, Y. Ganjali, "Protecting home user devices with an SDNbased firewall," IEEE Transactions on Consumer Electronics, vol. 64, no. 1, pp. 92-100, 2018.

[30]A. Rana, A. Raza, X. Z. Wang and et al., "Fuzziness based semisupervised learning approach for intrusion detection system," Information Sciences, vol. 378, pp. 484-497, 2016.

[31] F. Yousef, "How to secure web servers by the intrusion prevention system (IPS)", International Journal of Advanced Computer Research, vol. 6, no. 23, pp. 65-71, 2016.

[32] Y. Wang and J. Vassileva, "Bayesian network-based trust model," Proceedings IEEE/WIC International Conference on Web Intelligence (WI 2003), Halifax, NS, Canada, 2003, pp. 372-378, doi: 10.1109/WI.2003.1241218

Rahul Lal Radhakrishnan graduated B tech [Bachelor of Technology] in computer science engineering from MG university Kerala, India. His research interests are Network Security, Cybersecurity, commercial network routing, Industrial experience on web security, web analyst, web development fields

HALMSTAD UNIVERSITY

PO Box 823, SE-301 18 Halmstad
Phone: +35 46 16 71 00
E-mail: registrator@hh.se www.hh.se