QoS-AWARE FAULT DETECTION IN WIRELESS SENSOR NETWORK

Dissertation submitted in partial fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY
in

COMPUTER SCIENCE AND ENGINEERING

By

VAISHALI KALRA
(11209208)

Supervisor
RAVI KANT SAHU
(Asst. Professor)

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

May, 2017

ABSTRACT

Information plays an important role in today's world. For transmitting this information, we use a lot of different kind of network system. Among this the most widely used medium is the wireless sensor network. But due to the high end traffic of the transmission of this information, some failure takes place. Moreover, due to far deployment and small size of sensor nodes, energy consumption is the major issue of wireless sensor network. Detecting the node failure and retrieving the data associated with that faulty node is very important. To recover the data in the case of network failure, the technique of check pointing is proposed to choose the most suitable backup node for the data transmission to the base station.

DECLARATION

I hereby declare that the research work reported in the dissertation entitled "QoS-AWARE FAULT DETECTION IN WIRELESS SENSOR NETWORK" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Ravi Kant Sahu. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Vaishali Kalra

11209208

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**QoS-AWARE FAULT DETECTION IN WIRELESS SENSOR NETWORK"**, submitted by **Vaishali Kalra** at **Lovely Professional University, Phagwara, India** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Ravi Kant Sahu

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____
2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

It is not until you undertake research like this one that you realize how massive the effort it really is, or how much you must rely upon the selfless efforts and goodwill of others. I want to thank them all from the core of my heart.

I owe special words of thanks to my supervisor Mr. Ravi Kant Sahu for his vision, thoughtful counseling and encouragement for this research on "**QoS-Aware Fault Detection In Wireless Sensor Network**". I am also thankful to the teachers of the department for giving me the best knowledge guidance throughout the study of this research.

And last but not the least, I find no words to acknowledge the moral support rendered by my parents and moral support given by my friends in making the effort a success. All this has become reality because of their blessings and above all by the grace of almighty.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 WIRELESS SENSOR NETWORK

Wireless sensor network (WSN) consists of a huge number of tiny sensor nodes. Each sensor device has the capability to compute, communicate, sense and operate. Primarily, WSNs have been used widely in a variety of applications to perform tasks like environment monitoring and real time decision making. These tasks are purely dependent on the quality of data and information of the WSN.

Sensor nodes in the WSN are basically responsible for carrying up all the quality data and information. These sensor devices not only sense the situation but also cooperate with each other. So, sensing and communicating the data is the basic principle on which wireless sensor network works.

Besides sensor nodes, WSNs also contains sinks and sources. These all devices are connected with each other via wireless medium. This medium can be radio signals. These sensor devices are not expensive and are lower in energy. Moreover, these nodes have different memory capability. The sensor devices have functionality of sensing environmental and physical factors like pressure, temperature and sound in the field of network where they are actually deployed.

Hence, the nodes extract the data and information and then this is information is processed and is sent to the base station or central node via network. The nodes adjacent to a particular node are called its neighbor nodes. Every node passes the data to the next node. The next device then transfer the information to the neighbor node until it reaches the destination node.

To pass the information to the destination node, the sensor device should be aware about the direction of the destination node. While passing the data to the intermediate nodes in order to reach the destination node, the energy consumed is very high. Moreover, tasks like

sensing the environment and collecting the data also requires high amount of energy. WSNs have numerous characteristics which are as following:

- Wireless sensor network is scalable in nature which means that any number of nodes can be deployed at any point of time; hence wireless sensor network can be enlarged.
- It is very easy to set up or configure a wireless sensor network because node deployment is done without any sort of installation.
- There are tons of sensor devices deployed in a wireless sensor network.
- Wireless sensor network has a feature of node mobility.
- It creates a scenario where human's physical presence is not required.

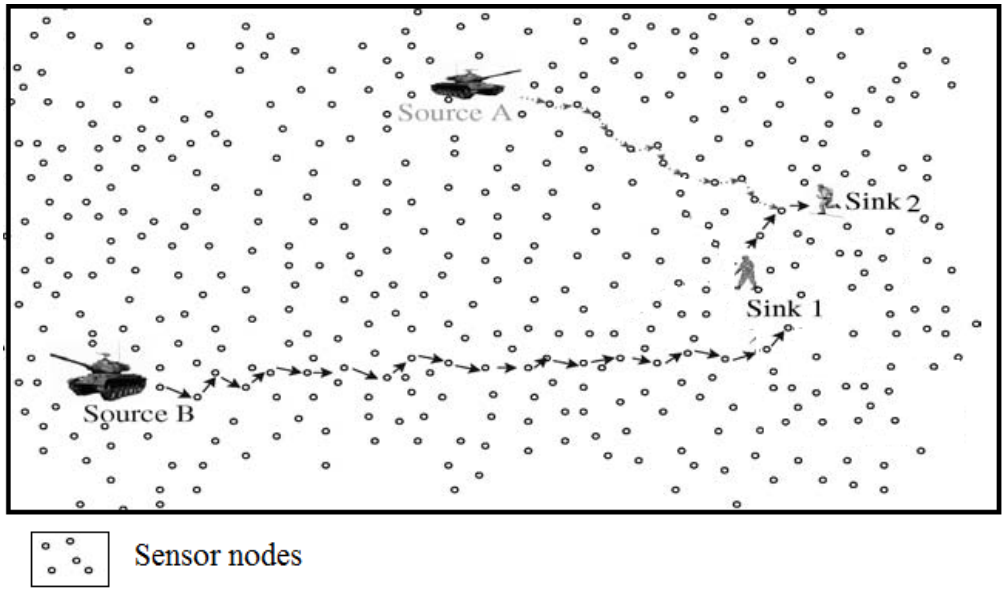


Figure 1.1 Wireless Sensor Network (WSN)

1.2 TYPES OF SENSING IN WSN

- Event Sensing: It is the sensing technique where only events are being sensed.
- Periodic Sensing: In periodic sensing, the queries and events are being sensed in a periodic manner.
- Query sensing: Query sensing is the sensing process where only queries are being sensed not the events.

1.3 SENSOR NODE

Sensor node is the very important and main element of a wireless sensor network. Their functionalities include sensing the events, gathering and processing the data, and then finally forwarding the information to the destination node via neighbor nodes in the field. Besides sensing and other activities, sensor nodes also send back queries to the source nodes generated by sink or base station. In all, the sensor nodes act as communication channel between source node and sink. Every sensor node in a wireless sensor network has following subsystems:

- Sensor Subsystem
- Processing Subsystem
- Communication Subsystem

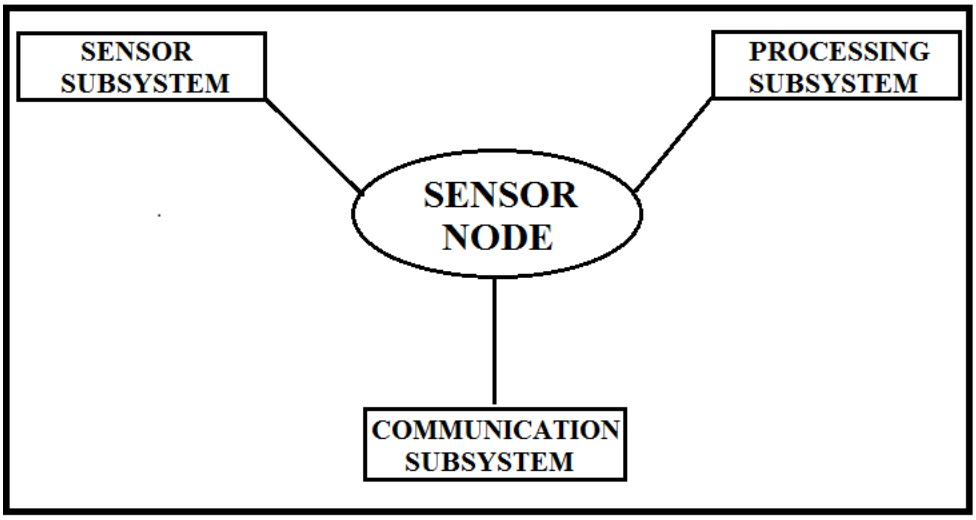


Figure 1.2 Subsystems of a Sensor Node

Sensor Subsystem: The main function of this sensor component is to sense the environmental conditions or the events of the particular field.

Processing Subsystem: Processing basically comprises of all the computing, processing and storage related work

Communication Subsystem: Communication is done between the sensor nodes, their immediate neighbors, source and the sink. Hence the information is communicated effectively with in the sensor network.

The terms source, event, sink/base station are defined as following:

Event: Event is nothing but the data which is actually being reported.

Source: The node in the WSN which is responsible for initiating the communication and generating the data.

Sink: The sink node is the node which shows interest in the data which is related to the event.

1.4 HARDWARE FOR WIRELESS SENSOR NETWORK

As discussed above, a sensor node consists of components like sensing unit, processing unit, power unit and a transceiver unit. Sensing unit consist of further two units: analog to digital converter (ADC) and sensors. A small storage unit is associated with the processing unit. The purpose of transceiver unit is to connect the node with the network. WSN's hardware also includes batteries, CPU, power switch, antenna, external power connector, etc.

1.5 ARCHITECTURE OF WIRELESS SENSOR NETWORK

The architecture of WSN explains the scenario that how field, source nodes, sensor nodes, sink are related to each other. It depicts how source node generates the message and then how this message is traversed through the network via neighbor nodes. In Fig. 1.3, it is shown that how source sends the announcement message to nearest dissemination node, how one dissemination node forwards the data to another dissemination node and finally the announcement message reaches to the sink.

The sink then sends the queries to the source and after receiving the response of those queries, it sends the complete information to the manager node through the internet. Manager node takes makes plans to take appropriate actions correspondent to the particular events that are sensed by the sensor nodes. The components that communication architecture of wireless sensor network includes:

- Sensor nodes

- Dissemination nodes
- Sink
- Manager node

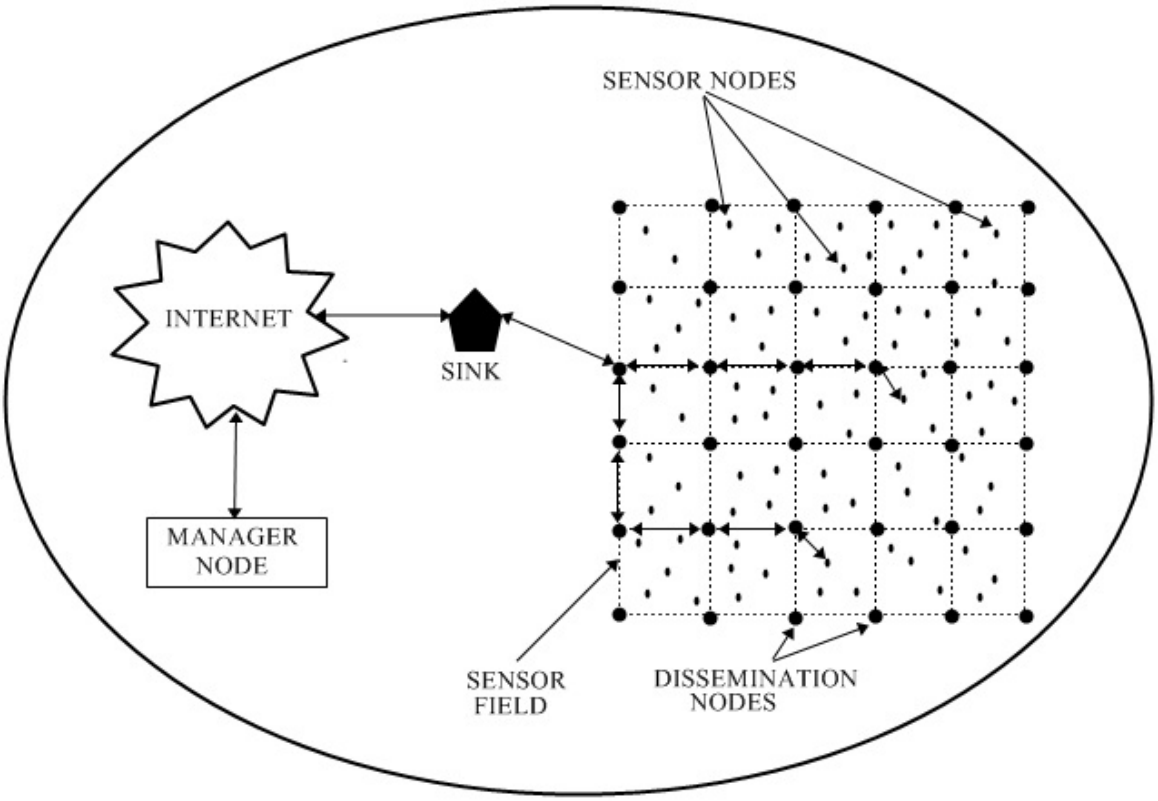


Figure 1.3 Wireless Sensor Network Communication Architecture

1.6 CHARACTERISTICS OF WIRELESS SENSOR NETWORK

There are various characteristics that differentiate the wireless sensor network from other networks. These characteristics are:

- Wireless sensor network consists of sensor nodes which are very small in size. So sensor nodes cannot de easily observed by the enemy.
- Sensor nodes are inexpensive.
- Wireless sensor network is application specific. So it can be deployed to perform any particular specific task.

- Wireless sensor network is data-centric as the communication in wireless sensor network is targeted to nodes in the given location.
- Wireless sensor network is self-organizing and self-configuring as the sensor nodes configure themselves at their own after deployment.
- Wireless sensor networks can be deployed in hostile environments where it's not so easy for the human to be present all the time.
- In wireless sensor network, nodes can be mobile.
- Wireless sensor network has the ability to cope up with the failures.

1.7 APPLICATIONS OF WIRELESS SENSOR NETWORK

The Wireless Sensor Network can screen an assortment of conditions in the distinctive environment like temperature, pressure, noise, movements, stress and so forth. So based on these conditions in which wireless sensor networks can be utilized we have a wide assortment of applications of these wireless sensor networks.

Military and Public-Protection Applications: Wireless Sensor Networks are utilized as a part of combat zone reconnaissance, checking and recognizing atomic and biochemical attacks. Such a wireless sensor network which is introduced for military and open security purposes ought to itself be shielded from gatecrashers, on the grounds that false disturbing of such a network will bring debilitating conditions up out in the open.

HealthCare Applications: Wireless Sensor Networks are utilized as a part of human services segment to screen the impact of medications and other related effects in patients by the specialist.

Scientific Applications: Wireless Sensor Networks are utilized by scientists to convey distinctive examination ventures. For instance the conduct of various winged animals are screen and identified by Wireless sensor networks

Engineering Applications: Many Engineering ventures use wireless sensor networks to screen the pressure, stress and distinctive ecological conditions like sensors utilized as a part of mechanical technology ventures.

Household Applications: Wireless sensors utilized as a part of a wide assortment in various house hold applications like clothes washer, microwave and so forth.

Environmental Applications: Wireless Sensors are used to monitor different environmental conditions like flood detection, soil and agriculture conditions and other different atmospheric conditions.

1.8 ISSUES OF WIRELESS SENSOR NETWORK

Although wireless sensor network has various unique characteristics but it also faces some challenges and issues. Some of the issues faced by wireless sensor network are:

Efficiency of Energy: Consumption of energy is an extremely fundamental component for the lifetime of the system. As the activity i.e. the transmissions of messages and queries between the source and the sink expands, more power is required. In the event that power utilization is builds the lifetime of the remote sensor arrange diminishes. So high power utilization is a snag for the lifetime of the sensor nodes and the remote sensor arrange.

Failure of nodes: Sensor nodes are inclined to disappointment as the of the nodes constantly diminishes. At the specific level the node come up short on the energy and it falls flat.

Unparalleled power sources: When the sensor node don't have energy, it goes down and it cannot be replaced with any other source of power.

Network failure: There are several nodes between source and the sink. So when the intermediate nodes between source and the base station actually fails then the communication can't be done between source and the sink. This results in sink isolation, which ultimately leads to network failure.

Storage issues: Sensor nodes are provided with very limited or less memory. So data stored is very limited in the sensor nodes.

1.9 FAULT TOLERANCE, DETECTION AND RECOVERY

Fault Tolerance: It is the property according to which a system work fines even if there is some occurrence of a failure or some components fail to work. It is basically a term which indicates the degree that how much a system can tolerate or bear a failure and continue to provide the services which it promised.so fault tolerance is a prime thing which is required in

the wireless sensor network. moreover, it is a mandatory in this kind of network because of sensor node properties, radio communications and tough environments in which these networks are being deployed.

Fault Detection: Fault detection is an approach in these kind of network in which the fault occur are traced and detected. Faults are classified as hardware faults or software faults. There are different approaches for finding faults in WSN.

Node Failure: Nodes in WSN are inclined to failure because of various factors like energy depletion, physical failure, announcement link errors, mischievous attack, and so on. Not at all like the cell systems and adhoc systems where vitality has no restrictions in base stations or batteries can be supplanted as required, hubs in sensor systems have extremely constrained vitality and their batteries can't for the most part be energized or supplanted because of antagonistic or unsafe conditions. In this way, one essential normal for sensor systems is the stringent power spending plan of remote sensor hubs.

Fault Recovery: Recovery is the process in which the faults detected are treated so as to make system fine. There are various proposed methods for fault recovery as well. This process involves cost, effort and time. Once failure is recovered, the system starts working correctly.

1.10 COMMUNICATION BETWEEN SENSOR NODE AND SINK

The movement in Wireless Sensor Network relies on upon number of queries created per Mean time. The sink node transmits the data to be detected by sending a query all through the sensor field. The sensor nodes react to the query by social event the data utilizing their sensors. At last when the sensor nodes have the consequence of the infused query will answer to the sink node through some directing convention. A sensor node likewise totals the answers to a solitary reaction which spares the quantity of packets to send back to the sink node.

1.11 LEACH PROTOCOL

The leach protocol is the protocol which is an energy efficient protocol which reduces energy consumption of wireless networks. In the LEACH protocol the overall network is divided into fixed size clusters and out of all those , cluster heads are selected in each cluster.

Cluster set up phase in this stage the every node portrays regardless of whether to wind up a cluster head for current round. Every one of the nodes pick a random number 0 or 1 for made a decision. A threshold worth is setup, if the quantity of the node is not as much as threshold quality, then the respective node turns into a cluster head for the existing or the current round.

Steady phase: The network will enter the steady stage when the cluster head dole out time slots to its individuals for utilizing TDMA mode. The steady stage is isolated into frame, where data is sent by the nodes to the CH at max once per frame amid their apportioned transmission slot. There are some deficiencies in choosing the cluster head in Leach for instance:

- There exists large and small clusters, simultaneously in the same network at same time.
- Sometimes, selection of the cluster head is not reasonable when the nodes are having different energies.
- When the cluster head becomes dead, then the other members of the cluster results in depleting energy.
- The algorithm doesn't consider the node location.
- Reasons for the failure of cluster head may be it doesn't focus on the geographical location , residual energy or other information.

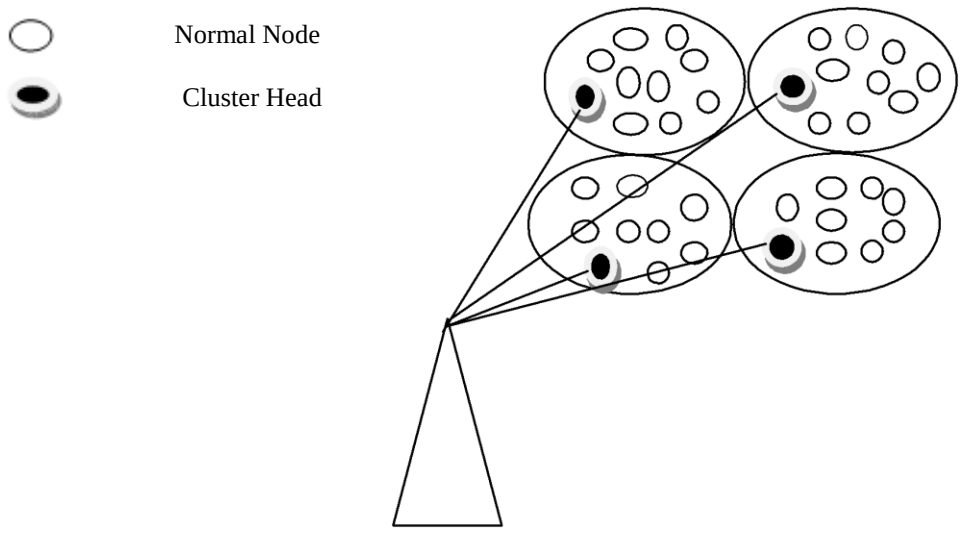


Figure 1.4 Clustering in Leach[9]

In the above figure 1.4, the LEACH is divided into three clusters. Black node is the cluster head which represent the cluster. All the white nodes are the members of the cluster these are not cluster head. The cluster head in a cluster is changed randomly by any cluster protocol. To changing the cluster head between each cluster nodes is to distribute the network load. In this way the performance of the entire network is improved and can be achieved lower energy consumption.

1.12 SECURITY GOALS OF WSN

Confidentiality: In Wireless sensor network the data is transmitted from one node to another node and after routing through many nodes, the data or information is conveyed to the base station. It is important that any message routed through wireless sensor network is confidential and not accessible to unauthorized user.

Authentication: It may possible that unauthorized access by some malicious node may drop some packets from network or may introduce some false packets into the network. Such unwanted affects can be avoided if we have some means to identify the original sensor nodes.

Integrity: The alteration done in data packets by malicious node violates the concept of integrity. Integrity means to ensure the correctness of the data. Receiver node should receive the data in original as send by the sender node.

Availability: Failure of a node may leads to failure of a path or failure of base station may leads to failure of entire networks. Sensor nodes and base station should always be available to provide services of Wireless sensor networks.

Freshness: The data of each message should have freshness i.e. data should be recent; no old data should be replayed by malicious nodes.

Time Synchronization: Most of the Wireless sensor network uses time synchronization to calculate the delay between packets in a pair of two nodes.

CHAPTER 2
REVIEW OF LITERATURE

This chapter observes the different types of methods which are developed for the fault detection in wireless sensor network. Mainly the wireless sensor network monitors the particular area on the basis of certain environmental and other factors. The main emphasis of this chapter is to survey the various protocols and algorithms designed with the purpose of detecting fault, improving quality factors and saving data in WSN.

2.1 LITERATURE REVIEW

The reviewed literature describes the various fault detection techniques various research papers have been reviewed to analyze the detection techniques and various ways through which energy can be saved. The various others factors which are focused are data efficiency, fault prevention, energy efficiency etc. The reviewed research papers are explained in this chapter.

Sandeep Saurav Singh *et.al* (2016), "Sensor Node Failure Detection using Check Point Recovery Algorithm" explains that using huge number of nodes in an application raises the Quality of service (Qos). Along with that using huge number of sensor nodes also causes failure thereby affecting the QoS. Failure of sensor node can occur because of various reasons like battery issues, environmental issues, physical or software problem.

For raising QoS one thing way too necessary to find the faulty node and retrieve the packets associated with that faulty sensor node. Current scenario uses Round Trip Delay (RTD) time for detecting the faulty node. [8]RTD is basically the actual time required to get the packet at receiver's end and receiving the acknowledgement at the sender's side. If RTD comes out to be greater than its normal value, in that case it is considered that the node has failed.

This has one problem that this scenario is not able to detect the fault at required time. Hence, it leads to loss of data in the network. To eliminate this problem, in this paper the Check Point Recovery Algorithm (CPRA) is proposed for fault detection. The CPRA finds

the energies value of each deployed node. At some period of time, all the sensor nodes will send a heartbeat, due to which we get to know that the node is working fine or not.

When the energy value of the node goes down it will not send any heartbeat to the checkpoint, due to which, we get to know that the node is leading towards failure. So, the data of the failed should be passed to some other node which will lead to an increase in the reliability of the system. An approach of Check Point recovery algorithm (CPRA) is suggested.

This paper also demonstrates an AODV (Ad-hoc On Demand Distance Vector) protocol to find the shortest path between two deployed nodes in the network. The Check Point Recovery Algorithm is implemented for detecting the malicious nodes.

If the heart beat is not gotten by a specific node, it implies that that the level of energy of that particular node is way too low and it is driving towards failure. At the point when the node with low level of energy is identified, it is supplanted by another node. Dynamic sensor nde is utilized for supplanting the node whose vitality level of energy is going to deplete with another node whose level of energy is high to keep the node safe from getting failed. The Network Topology Management (NTM) helps in building up the connections of the node which replaces the faulty sensor node..

After the substitution of the nodes, the ID of the supplanted node will be communicated to all the neighboring sensor nodes. In case the nodes are already supplanted before going into the failed state, then the information related with that node won't be lost. This reduces the information loss in the framework and along these lines, expanding the effectiveness of the framework.

Deepak Nandal *et.al* (2016), "Fault detection in wireless sensor network" explains that WSN is the configuration which includes communication elements. The controllers of WSN work on monitoring these networks. As nothing is perfect, so there is chance of failure in WSN too. These failures are because of the faults occurring in WSN[7].

So this article has mentioned about the detection, diagnosis and recovery of these faults. Its applications are monitoring military operations and critical infrastructures, data acquisition in hazardous environment, environment applications, automated building climate

control, habitat, civil health observing, industrial process observing, and quick energy responses.

Furthermore, the need of development is explained that is growing advancement of technology has expressed the need of developing sensors. So there is a need of wireless sensor network to connect these independent sensor devices. WSN are vulnerable to failures, so thats is important to find the faulty nodes and working nodes.

How it works: As mentioned above WSN is a network of independent sensor devices/ nodes which communicate through wireless links. WSN are self-healing and self-organising. Self-organizing: In this a node spontaneously joins a node devoid of any manual help. Self-healing: It works in case of failure, if nodes get faulty, the communication bythe nodes can be done through alternative paths. The components are actuators, memory, sensors and controllers, communication, battery. The categories of WSNs are earthly WSNs, underwater WSNs, underground WSNs, mobile WSNs, multimedia WSNs. Types of faults hard faults, soft faults.

Fault management process involves detection of faults, then fault is diagnosed, fault recovery. In fault detection, two approaches have been followed that is centralized and distributed. In centralized, there is a centralized sensor node which monitors and takes responsibility for finding the faulty nodes. Whereas in distributed approach, decisions are made level wise before it communicates with the central node.

Node Self Detection: In this self-detection of the node failure is done by the node where node just sees the binary output of the sensors by relating it with the pre-available fault models. Neighbor coordination as the name suggests the neighbors are involved to detect the network faults before going to the central node. This paper has also mentioned the method for fault detection:

In clustering there is a cluster head out of N nodes. The burden of the cluster node has to be minimized. To minimize the load of a cluster node, relay nodes is introduced between head and sink whose performance is well than cluster head and cluster node. Cluster head will be elected on the basis of availability of higher energy. The poison distribution is used to

identify faulty nodes. It will calc. he failure probability. A scheme of poison failure density is proposed.

Distributed reference fault detection Algorithm: Based on the pair wise output of the sensor, if output comes out same then linear relationship exists. Due to scalability the failure increases. In this method no need to have complete knowledge of system input. It can be performed in decentralized way due to the pairwise nature. So it is energy saving as compare to centralize.

Improved Distributed Fault Detection Scheme (DFD): It detects the futile nodes by swapping information and communally testing amongst neighbor nodes in the network.

The Disadvantage can be, earlier DFD scheme's performance decreases when neighbor nodes are small and node failure ratio is high, but improved DFD works in wireless sensor network too with small neighbor nodes and higher failure ratio.

Sirajul Ameen *et.al* (2014), "Fault Tolerance Using Cluster in Wireless Sensor Network" The focus of this paper is to minimize the task of cluster head. A group of nodes is called a cluster. Cluster head is chosen on basis of forte node and they pass data ultimately to sink node. [3]These nodes sense the atmosphere and cooperate with each other, after that generate a value as global consequence that will pass the status to sink node in the network. Fault tolerance: Nodes respond to the input without getting fail.

Even if one of the nodes gets down, the system as a whole doesn't get affected. Fault diagnosis: Failures are of two type hardware and software faults. Fault can either occur if node gets out of range or some get down due to battery weaknesses. Problematic scenario: cluster nodes direct the information data to cluster head in order to send data ultimately to sink node, cluster head keep passing data to the nearest cluster heads and this may result early battery drain of cluster head.

Model communication: burden is reduced by introducing the relay node between head and sink. Before transmission, record the Battery life, one with the highest is the cluster head. Features of relay node are as following:

- More battery strength

- 1 mb flash
- 64 mb SD Ram
- 400 mhz linux system
- Relay node is responsible for data packet fusion from sensor nodes.
- Sensor nodes are responsible for sensing the information from a respective clusters after that transmitting to destination via multipath
- Communication is done by RCS (radio communication section), this section increases energy to do task.
- Similarly, IRS (information recording section), to store information received from previous node.
- ICS (information conventional section), decides what to forward next.

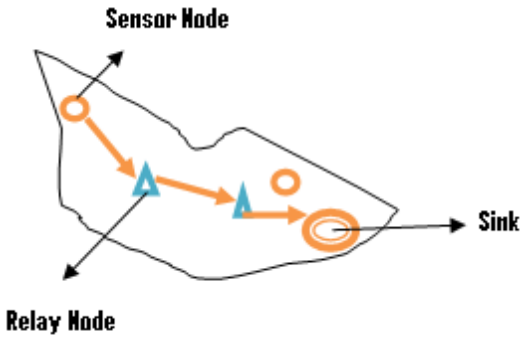


Figure 2.1 A simple architecture of a relay node[3]

Besides above all, the algorithm of Poisson distribution is explained in this paper.

C.Ahila Jerlin *et.al* (2016), "Fault Tolerance In Wireless Sensor Networks" explains that an main problem amongst the various design dares in building up sensor nodes is to guarantee that multi nodes are having a whole network wide communication between them, each with limited Trans processing capabilities and having a shared communication channel[4].

A great effort has already been used in creating control over topology and various strategies for routing to decrease the communication overhead and ensuring proper delivery of the message. This paper has explained about the hardware required for a wireless sensor node. It has also described about the functioning of various subunits like processing unit, storage unit, etc. Furthermore, the concept of node failure has been explained.

Not at all like the cell systems and specially adhoc systems in which energy has no restrictions in base stations or batteries can be replaced as required, nodes in sensor systems have exceptionally constrained energy and their batteries can't get recharged or supplanted because of threatening or dangerous situations. The process which implemented in sector is automatic fault Recovery when a mica motes connected in a certain topology the signal which may transmitted to a particular level of the frequency the frequency of the mote is 2.4ghz and finally.

Motes are transmitted the data to the base station if one mote is under malfunctioning in the transmission path. Finally the path of transmission of destination to source is assigned through shortest distance between one node to another node. In this paper, author has given a fault tolerant strategy for multi path routing and energy efficient wireless sensor network (FTMRS). The FTMRS also recommends a strategy for faulty node recovery that effectively replaces the node having failure. The results of the simulation comes up with the result that proposes scheme of routing which gives better observing of the nodes that viably prompts a good fault tolerant scheme energy efficiency wise.

Ehsan Warriach *et.al* (2012), "Fault Detection in Wireless Sensor Networks: A Hybrid Approach" explains about three detection approaches. Author has given three qualitatively methods Markov Model (HMM - learning-based)[5], Linear Least-Square Estimation (LLSE) and rule based to define rules for detecting faults and failures dynamically.

Rule based schemes are basically lies under domain and expert knowledge to characterize heuristic guidelines for distinguishing faults. Estimation techniques foresee typical behavior of the sensor by utilizing sensor relationship. At last, learning-based strategies can measurably recognize and arrange classes of faults. The system heuristics rules based on

In this paper the terms like noise, outlier, short, and constant have been explained. Short: first of all, the physical behavior between two nodes is sensed and then the rate of change of this phenomenon is calculated. This calculated rate is then compared to the the threshold value, if the rate is low than that of threshold then it is considered that short fault is occurred.

In short faults, the occurrence of faulty readings is more often. LLSE and HMM methods, and a Hybrid (combination of Rule, LLSE and HMM) method is applied so as to detect the short faults. In all, a hybrid approach is suggested by the author to detect the faults and also there is plan to integrate this model with the mathematical models for fault detection.

Zhaoxing Wang *et.al* (2012), "A Fault Detection Scheme Based On Self-clustering Nodes Sets for Wireless Sensor Networks" have presented a fault detection scheme based on self-clustering nodes sets for wireless sensor networks. [2]Let us consider a network where n number of sensor nodes are deployed. The purpose is to gather the sensing data over this region. If the data gathered doesn't lies under normal limit, then a alarm is triggered.

The sole reason of this paper is to detect the faulty sensor nodes. The normal node can be a one having some measurement errors or having transient faults but the nodes having permanent communication fault has to be chucked out of the network. They are no longer eligible for the network. Clustering means grouping of the nodes or entities having similar properties or behavior. Hierarchical clustering is a part or method of clustering methodology in which a hierarchy of clusters is made.

The hierarchical clustering is distinguished in two ways. One is agglomerative which means bottom up method. In this method hierarchy goes from bottom to top. The clusters on the lower levels are merged first and then moves upwards. Whereas the second approach is

Top down approach which goes from top to bottom.

Based on the similar behavior of the nodes, the clustering algorithm is used in this paper. Furthermore, we utilize the agglomerative approach. Keeping in mind the end goal to choose which groups ought to be joined (for agglomerative), a measure of uniqueness between sets of perceptions is required. In many strategies for various leveled grouping, this is accomplished by utilization of a suitable metric (a measure of separation between sets of

perceptions), and a linkage paradigm which indicates the divergence of sets as a component of observations of pair based distances.

In this phenomena , this distance factor is used to calculate the dissimilarity factor between . And we calculate the sum of Nodes numbers of the top three large-scale sets, when the sum accounts for greater than of all nodes, clustering is stoped.

Sutharshan Rajasegarar *et.al* (2008), "Anomaly Detection in Wireless Sensor Networks" explains about Anomaly detection in wireless sensor networks which involves intrusion detection, fault diagnosis and monitoring applications. The main focus is on how to reduce or to minimize the energy ingestion in sensor nodes and to maximize the life of the network[1]. The important terms are:

- Anomaly– Anomaly can be called as outlier. The inconsistent behavior of the data set.
- Intrusion Detection- Analyzing and identifying the malicious activities.
- Wormholes– In this, an atrractive path is created by two nodes and whole network traffic is tunneled through that.
- Stochastic process- Probabilistic or random process.

Applications mentioned in the paper are:

- Intrusion detection- It helps in detecting several types of attacks. The major issue in this is to find out the way by which we can reduce false alarms.
- It helps to find the uncommon changes in the network.
- To eliminate the erroneous measurements from sensors in order to avoid faults.

Authors have further mentioned the two broad techniques of anomaly detection:

- Statistical Technique: In this technique, the prior information or knowledge about the distribution of the given data is known. Disadvantage of this methodology is that it causes complexity due to huge number of parameters which are to be calculated.
- Non parametric techniques: In this technique, the distribution of data set is not known. The Non Parametric approaches are further classified as:

Rule based approach: There are certain predefined rules. If the rules applied result in anomalous condition, then the anomaly is detected. Rules can be integrity rule, retransmission rule and repetition rule.

CUSUM approach: This approach is used to find change in the mean value of probabilistic or random process. Anomaly is detected by comparing the CUSUM value to the threshold value. The disadvantage of CUSUM approach is that a greater value of threshold will result in more detection delays. The other one is that it only focuses on features in isolation. The advantage is that it detects attacks like wormhole, sinkhole and jamming.

Data clustering: Here the clusters of data points with similar properties are built. Points lie outside these clusters are termed as outliers. It detects routing attacks in sensor networks.

Density based approach: In this method the population density distribution of the data is measured and data values lying in the low dense regions are termed as outliers.

Support vector machine: In this method hyper sphere of the data vector is made. The data that lie outside the hyper sphere is termed as anomalous data. Here we have the problem of communication overhead.

Comparison of above approaches is as following:

- Statistical approach offers better detection performance when data distribution is known.
- Non parametric technique is efficient when distribution is unknown and environment is dynamic.
- The computational complexity comes from rule method to CUSUM approach, clustering method, density and the SVM approach.

Alessandra De Paola *et.al* (2013), "QoS-Aware Fault Detection in Wireless Sensor Networks" raised a real critical problem that is to find or keep a track of corrupted values of the readings amongst the huge amount of collected sensed data. such readings affect the wireless network, so it is mandatory and highly advisable to remove them. This problem is resolved by fault detection methodologies that are categorized by temporal and spatial

correlations[6]. These algorithms does not considers QoS requirements other than the classification accuracy.

A completely appropriated calculation for identifying information deficiencies, considering the reaction time other than the order exactness. They embrace the Bayesian systems to perform order of readings and the Pareto improvement to enable QoS necessities to be all the while fulfilled. Their approach has been tried on a manufactured dataset keeping in mind the end goal to assess its conduct concerning diverse estimations of QoS limitations. The exploratory assessment created great outcomes, demonstrating that calculation can enormously lessen the reaction time at the cost of a little diminishment in arrangement precision.

The distributed QoS-aware fault detection algorithm (QAFD) is composed of two main building blocks a fault detection algorithm, based on the Bayesian networks, and a QoS-aware optimization algorithm, periodically affecting the structure of the Bayesian networks. A great weakness for each of the described approaches is that they present a fixed computational complexity, strictly dependent from the adopted method; the computational complexity highly affects the ideal upper bound of classification accuracy. As a consequence, in noisy scenarios or when achieving a high classification accuracy is very important, it is suitable to adopt a more precise approach, even if it is more resource demanding.

This paper proposed a distributed fault detection algorithm for WSN, which is able to find the optimal trade-off among different and possibly contrasting QoS requirements. Even if we considered only classification accuracy and response time, many other QoS requirements could be considered, provided that the corresponding metric is defined.

Ravindra Navanath Duche *et.al* (2014), "Sensor Node Failure Detection Based on Round Trip Delay and Path in WSNs sensors" has proposed a fault detection method which is based upon the calculation of RTD. This RTD that is round trip delay is compared to a threshold value. The problem lies in this concept is that the detection of the faulty node is done when the calculated after RTD surpasses. So due to this limitation the data related to that failed node is never recollected again and is lost.

K. Sha *et.al* (2013), "Multipath routing techniques in wireless sensor networks" has proposed a cutting edge overview of current multipath steering conventions for WSNs, which are characterized into following three classifications, non-infrastructure based, coding based and foundation based, in view of the uncommon strategies utilized as a part of building numerous ways and conveying detecting information.

LI Jian-qi *et.al* (2013), "Energy optimized approach based on clustering routing protocol for wireless sensor networks" proposed enhanced clustering routing calculation which needs energy efficiency. To begin with, choose a cluster head by the energy factor[13]. After that observe the internal architecture of the cluster by determining the snugness coefficient of each cluster and then upgrade the communication way among cluster heads by enhanced multi-objective swarm calculation.

Nicolas Gouvy *et.al* (2013), "Energy efficient multi-flow routing in mobile Sensor Networks" proposed PAMAL (PATH MERGING ALGORITHM) new topographies routing calculation for mobile node .the proposed first routing protocol which is found and utilizes cross path method to adapt the topology to decrease the network congestion thusly while still upgrade energy efficiency[11]. The protocol makes the intersection to move far from the destination, getting nearer to the sources, ensuring more data aggregation plus saving the energy. It enhances the network life time 37% than existing.

Y. Jennifer *et.al* (2008), "Wireless sensor network survey" discussed the survey report is based on wireless sensor networks. The sensors are smaller, cheaper and intelligent device. For communication purpose we equipped it with wireless network[12]. The design of a network depends on its significant applications and not just limited to military tracking, surveillance, environmental monitoring, industrial machine monitoring.

B. Alakesh *et.al* (2014), "A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks" explains a brief introduction to routing protocol challenges in WSN along with some basic issues related to designing the routing protocols. The basic ordering of routing protocols in WSNs according to the most energy efficient protocol named LEACH describe with its advantages and disadvantages[15]. They also high light on some of the improve version of LEACH protocol.

U. Hari *et.al* (2013), "A Comparative Study of ACO, GA and SA for Solving Travelling Salesman Problem" proposed approach is to reduce the energy usage of network by using multi-hop routing process plus making use of Dijkstra's shortest path algorithm for data transmission. Proposed algorithm[16] use unequal size cluster concept with attributes like distance between nodes and base station, degree of nodes and results shows it improve networks life time and performance matrix.

S. Haidar *et.al* (2014), "An energy efficient Genetic Algorithm based approach for sensor-to-sink binding in multi-sink wireless sensor networks" proposed highly conserved to increase the lifetime of WSN. One method is deployed the multiple sinks, which are way more capable as compare to sensors[23]. These increased the area coverage and reduce the communication link between sensors and base station.

This give rise to a problem which sensor should bind to which sink in order to avoid. Over- loading on sinks. A Genetic Algorithm type approach was used to resolve the balancing problem. For further work in the future in this paper we have to do more things like introduce the concept of non-exclusive nodes to neighbor sensors, analyzing the routing oath failure and path recovery solution in multi-hop approach.

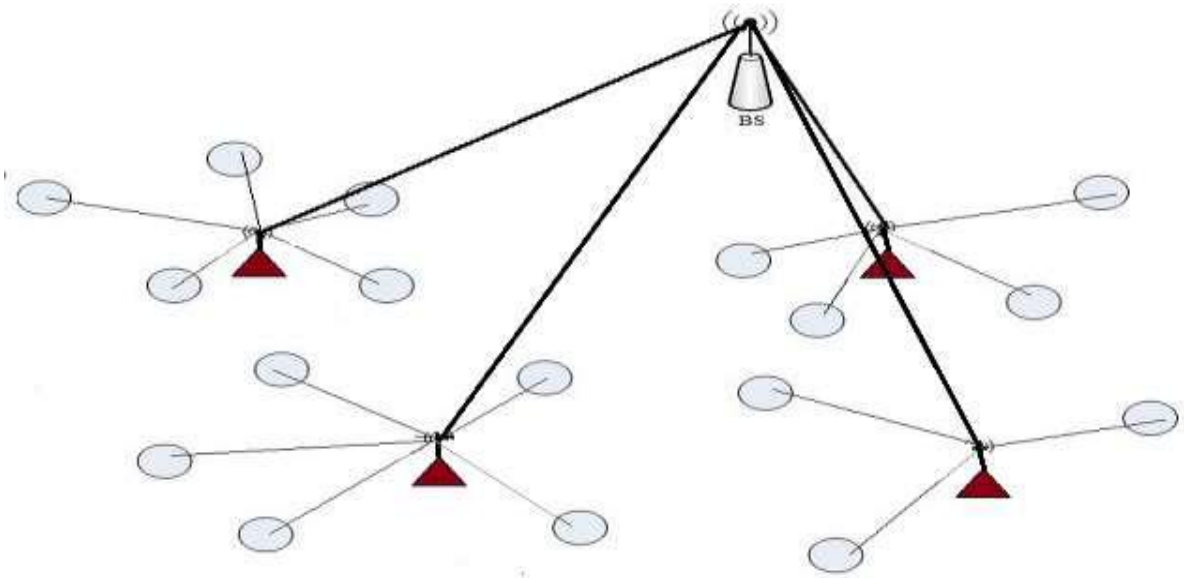


Figure 2.2 Wireless Sensor Network with Multiple sink[23]

S. Rajasegarar *et.al* (2013), "Distributed Anomaly Detection in Wireless Sensor Networks," proposed a distributed fault detection technique which is solely similar to clustering. Wireless sensor networks with a hierarchical topology are taken care of. In a centralized approach, every sensor node provide their data measurements to the gateway node and then an anomaly detection algorithm is run on the combined data at the gateway node to detect faults[24]. This method is greatly useless performance wise and also doesn't justifies the communication overhead incurred in the network.

2.2 TABULATED COMPARISON

Table 2.1 Tabulated Comparison

PAPER	TECHNIQUE	ADVANTAGES	DISADVANTAGES
Sensor Node Failure detection using check point recovery algorithm.	RTD, CPRA	Enhances QoS, detects faulty node,	Data packet loss, data recovery overhead
Fault Tolerance Using Cluster in Wireless Sensor Network	Burden of cluster head is reduced by introducing the relay node between head and sink.	Minimize the task of cluster head.	Cluster head keep passing data to the nearest cluster heads and this may result early battery drain of cluster head.
Sensor Node Failure Detection Based on Round Trip Delay and Path in WSNs sensors	Round Trip Delay (RTD) time of discrete round trip paths are used for the detection of faulty nodes	Detects the malicious node	Node detection occurs after the RTD gets over. The data related to that node is lost and can't be recovered leading to packet loss
Anomaly Detection in Wireless Sensor Networks	Statistical techniques and non-parametric approaches are explained	Minimize the energy consumed in sensor nodes and to maximize the network lifetime.	Statistical approach offers better detection performance when data distribution is known.

CHAPTER 3
PRESENT WORK

3.1 PROBLEM FORMULATION

Wireless Sensor Networks have numerous sensor nodes within, which are spread randomly over a region for several applications. WSN can become prone of Denial of Service (DoS) attacks, in which cause data loss along with energy expenditure.

In this work, network has finite number of sensor nodes and using leach protocol whole network is divided into fixed size clusters. The cluster heads are selected in each cluster on the basis of distance and energy.

The shortest path will be established from source to destination on the basis of reactive routing protocol. In this network some malicious nodes may join the network which reduces the network performance. The wireless sensor networks is the decentralized type of network due to which node failure chances are very high.

In the base paper, technique of check pointing is been proposed in which sensor nodes maintains the check point on the node which has maximum trust value. To increase the performance of the base paper algorithm, need to add some parameters of the wireless sensor networks to reduce chances of failure.

3.2 OBJECTIVES

1. To study and analyze the data backup technique for wireless sensor networks
2. To propose improvement in the check pointing based algorithm to reduce chances of node failure in the network
3. The proposed improvement will be based on to add trust parameter for the calculation of based node to maintain check points
4. Implement proposed algorithm and compare with existing in terms of various parameters

3.3 RESEARCH METHODOLOGY

The wireless sensor networks are the type of network in which sensor nodes sense the environmental conditions and communicate the sensed data to base station. The sensor network is deployed on the far places like forest, deserts etc.

The size of the sensor network is very small due to which its battery is very limited, due to far deployment of the sensor nodes it is very tough to recharge or replace battery of the sensor nodes. now a days, various approaches have been proposed which decreases the energy consumed by the network.

Among the various proposed techniques, the clustering is the most efficient technique in which whole network is partitioned into fixed size clusters and in each cluster, cluster heads are selected. The cluster heads are selected on the basis of energy and distance.

The sensor node which has maximum battery and minimum distance from the other nodes are selected as the cluster head. The sensor nodes in the cluster will aggregate its data to its cluster head. The cluster heads will communicate with each other and pass the data to the base station.

Due to self-configuring nature of the network and small size of the sensor nodes the chances of fault in the network is high which reduce efficiency of the network. The technique of back-up node is implemented which reduce the chances of fault occurrence in the network. In this base paper, technique the check pointing technique is been proposed in which node which has maximum trust value that node will be chosen as the best node to maintain check points.

To increase the efficiency of check pointing algorithm following steps are implemented in the research methodology:-

1. The network is set up with the fixed number of sensor nodes and whole network is divided into fixed clusters.

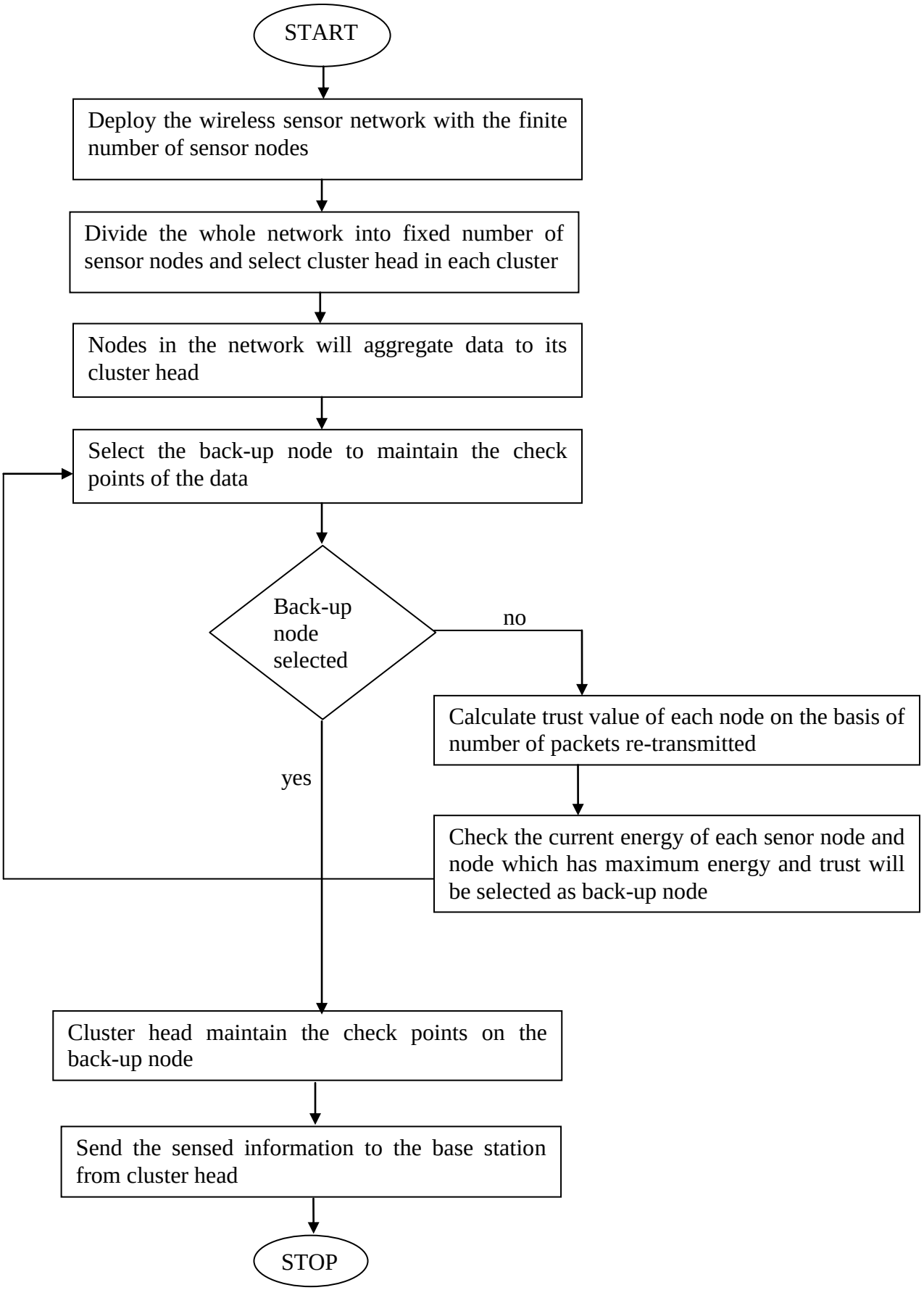
2. The cluster head gets selected in each cluster on the basis of distance and energy. The sensor node which has maximum energy and minimum distance from the other node is to be elected as the cluster head.

3. The back-up node is selected in the network on the basis of trust value which is calculated on the basis of number of packets re-transmitted in the network. The second factor is the energy, the sensor node which has maximum trust value and energy will be selected as the best node to maintain data back-up.

4. The cluster head maintain the data back-up on the node which is chosen as the data back-up node with the check pointing algorithm.

Proposed Algorithm

1. Select any sensor nodes from the sensor networks with M malicious nodes
2. Calculate trust of each node()
    1. Trust =number of packets retransmitted in time T
3. Calculate energy of each node
4. If Node has higher energy has threshold
5. Failure ==false ;
6. Then
7. Collect data from the normal node
8. Else
9. Failure =true
10. Check trust level of each node
11. Node (i)=Node which has maximum trust level
12. Back up the data to that Node(i) using check pointing
13. Goto step 1
14. Select the recovery node ()
15. The node which has maximum resources in terms of buffer size is selected as recovery node
16. After selection of recovery node broadcast the id to normal nodes
17. Stop


START
Deploy the wireless sensor network with the finite number of sensor nodes
Divide the whole network into fixed number of sensor nodes and select cluster head in each cluster
Nodes in the network will aggregate data to its cluster head
Select the back-up node to maintain the check points of the data
Back-up node selected
no
yes
Calculate trust value of each node on the basis of number of packets re-transmitted
Check the current energy of each senor node and node which has maximum energy and trust will be selected as back-up node
Cluster head maintain the check points on the back-up node
Send the sensed information to the base station from cluster head
STOP

As per the flow chart above, sensor network is deployed with n number of sensor nodes. The task of these nodes is to carry the transmission of data packets throughout the network. Nodes are divided into various clusters. In each cluster, a cluster head is appointed.

All the nodes in a particular cluster pass the data to its cluster head. Then the cluster heads of each cluster further pass the data packets aggregated at it to the base station. Before moving ahead, the term back up node should be clear to us. Back up node is the node which is responsible to recover the data from the failed node. Next step is to select the backup node to maintain the checkpoints of data. According to flow chart, if the backup node is selected then cluster head maintain the checkpoint on it and the data will be sent to sink by the cluster head. In case if the backup node is not selected then a new parameter that is trust value is calculated of every node. The meaning of trust value is number of packets retransmitted. Besides calculating trust value, the energy of every node is also calculated. The node having higher trust value as well energy value will be selected as the backup node.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 IMPLEMENTATION FRAMEWORK

The simulation is the technique which is applied to analyze the performance of the model which you have developed when actually it is implemented in the real time environment. The simulators are of two type, the first type of event based simulator and second type is time based simulators. The network simulator version two is the event based simulator in which created events are trigger on the defined amount of time.

The Network simulator is the simulator which is used to simulate the network models. The network simulator has various version and latest version is NS2-2.35 which is best compatible with ubuntu 12.04. The networks simulator version 2 is the linux based simulator which run on various of linux like fedora, red hat etc.

The NS2 is the complex architecture in which tool commands language is used for the front end and for the backend C++ is used as programming language. The performance analysis tools are used with NS2 and these tools are xgraph, ngraphs etc. The tool command language and C++ when used parallel it is called object oriented tool commands language. The NS2 is the only simulator which provides both type of text based and animation based simulation.

When the object oriented language is executed it gave two output, the first output is the .tr file which is called trace file in which output of text based simulation is saved, second file is .nam file which provides animation based simulation. The xgraph tool take the input of the trace files and generates the line graphs through which we can analyze network performance in terms of throughput, delay, bandwidth consumption etc.

To analyze the network performance C++ scripts are created and main trace file is given as input which gave numeric results in terms of throughput, delay, bandwidth consumption etc . The NS2 is the widely used simulator because it is the only simulator which provides both type of text based and animation based simulations

The proposed technique is been implemented in NS2 by considering the parameters given in table 4.1. It has defined the value of the parameters like which channel has to be used for the communication, the propagation model to be adopted, queue, antenna, area specified, number of nodes to be deployed in the network, frequency and the range used.

Table 4.1 Parameter values

Parameter	**Value**
Channel	Wireless channel
Propagation Model	Two ray model
Queue	Priority queue
Antenna	Omni directional
Area	800*800 meter
Number of nodes	37
Frequency	2.4 Ghz
Range	18 meter

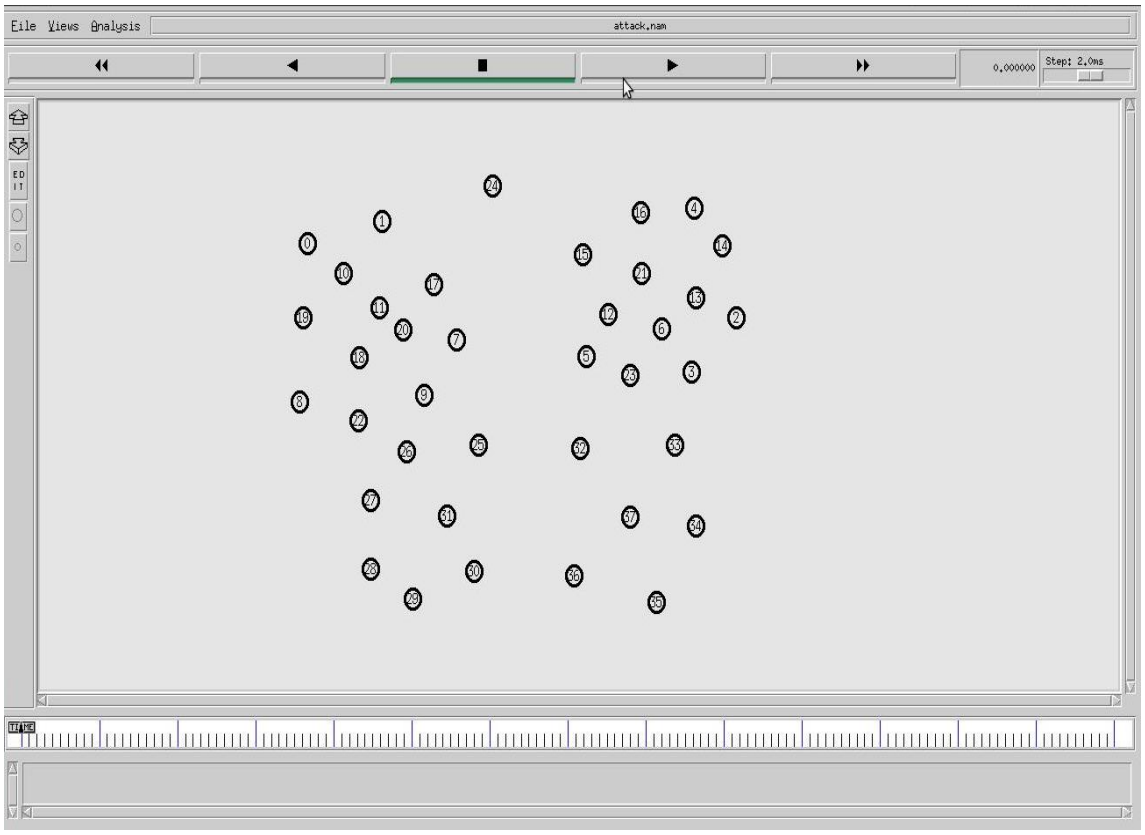


Figure 4.1 Network Deployment

As shown in figure 4.1, the network is deployed with the fixed number of sensor nodes. The whole network is partitioned into fixed size clusters. The location based clustering is applied to cluster the whole network.

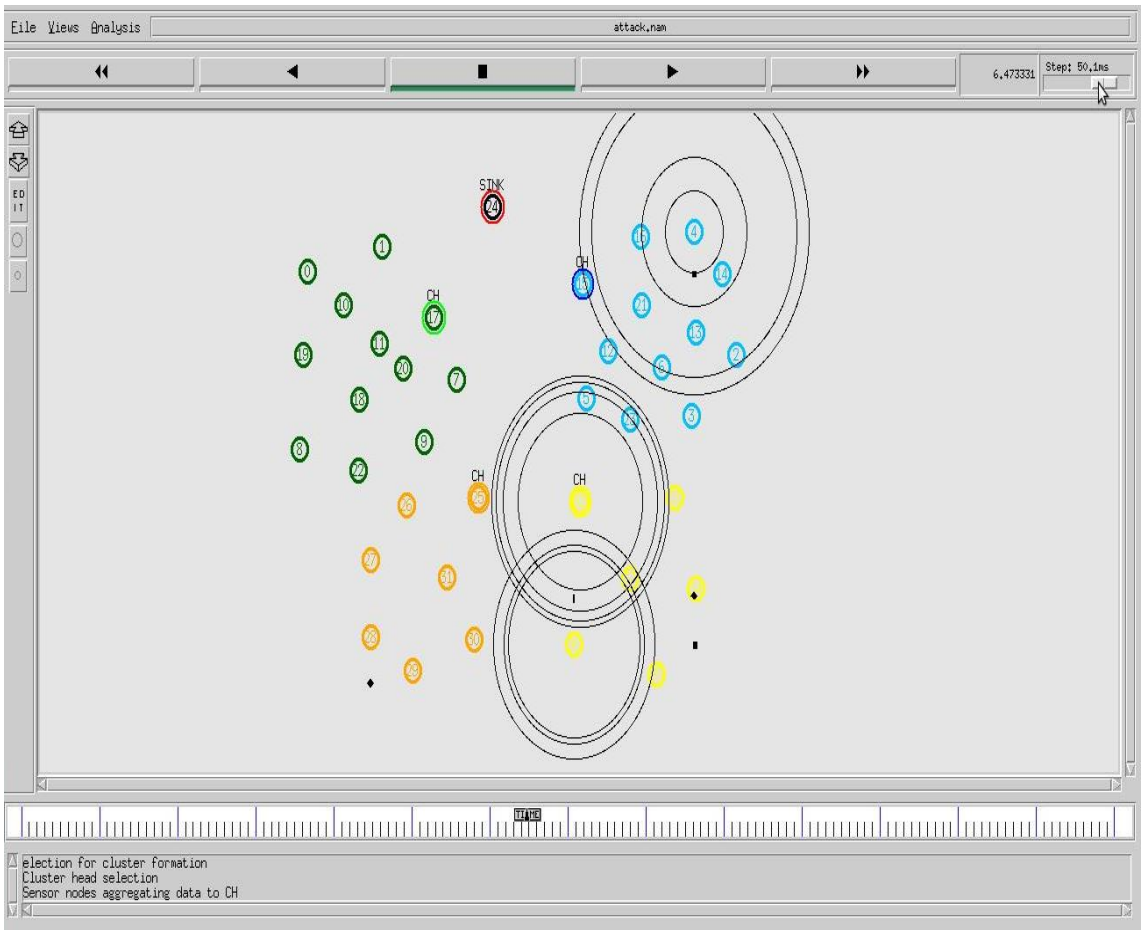


Figure 4.2 Clustering

As shown in figure 4.2, specific number of sensor nodes are deloyed in the given network. The whole network is partitoned into fixed size clusters. The location based clustering is applied to cluster the whole network .The LEACH protocol is applied to select cluster head in each cluster, the cluster heads are elected on the basis of distance and energy.

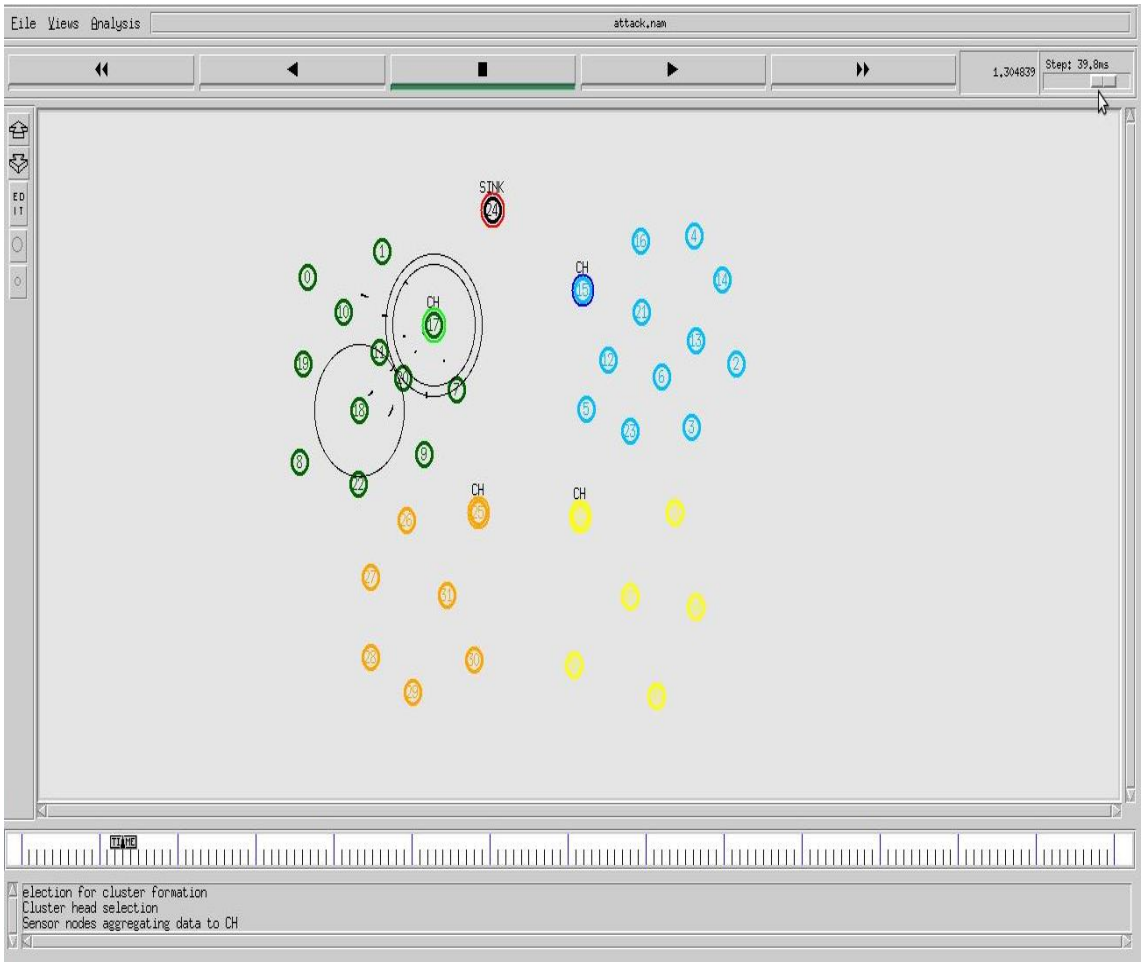


Figure 4.3 Data Aggregation

As shown in figure 4.3, the network is deployed with the finite number of sensor nodes. The whole network is divided into fixed size clusters . The location based clustering is applied to cluster the whole network .The LEACH protocol is applied to select cluster head in each cluster, the cluster heads are selected on the basis of distance and energy . The nodes in the cluster will aggregate its data to the cluster head. The required data will be transmitted to base station by the cluster head.

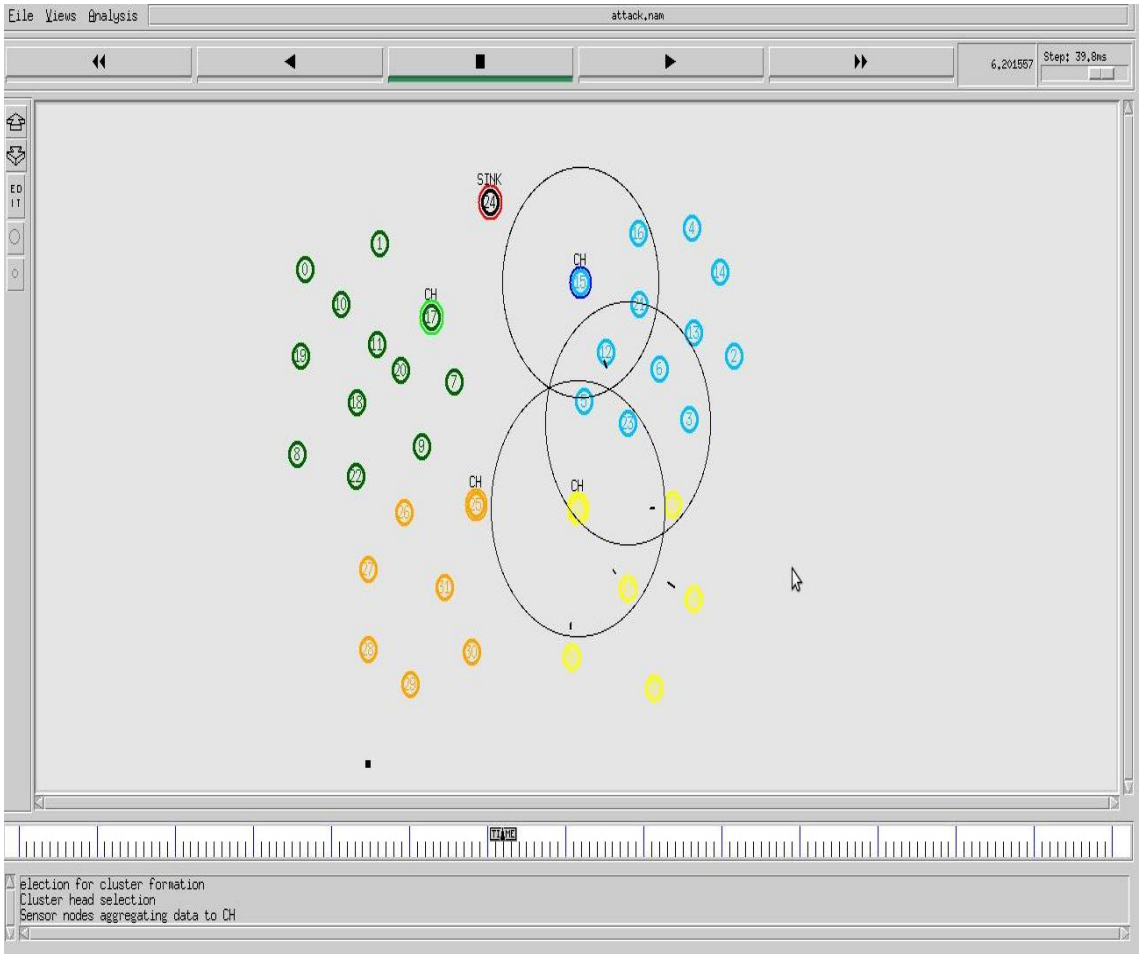


Figure 4.4 Data Aggregation contd.

As shown in figure 4.4, the data is aggregated on the selected cluster head of a particular cluster by the n cluster nodes. Once cluster heads gets the data from sensor nodes of its corresponding cluster, then the data is passed further to the sink node.

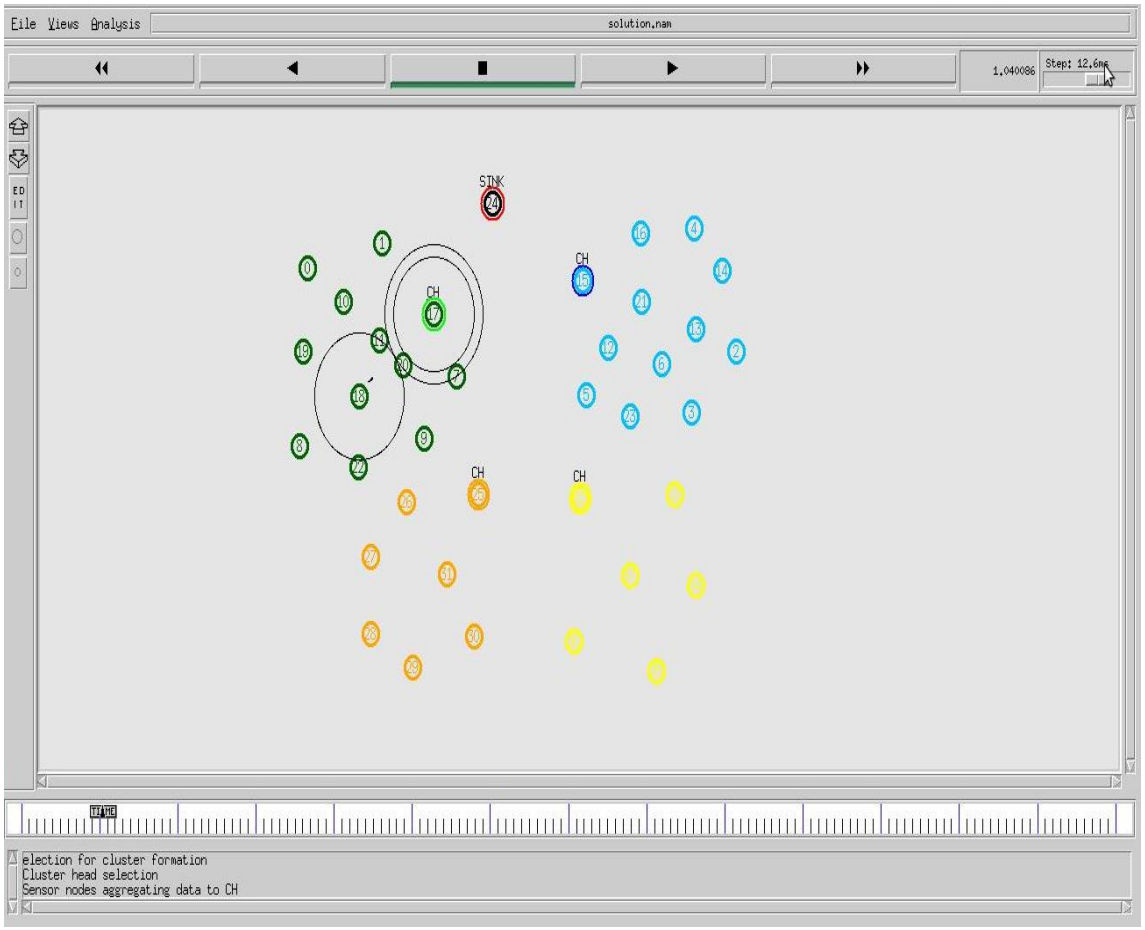


Figure 4.5 Energy Calculation

As shown in figure 4.5, The network contains finite number of sensor nodes and whole network is distributed into fixed size clusters using location based clustering. The technique of LEACH protocol is applied to select cluster head in each cluster. The best path will be selected to base station from cluster. The current energy of every node is calculated for the selection of most efficient back-up node.

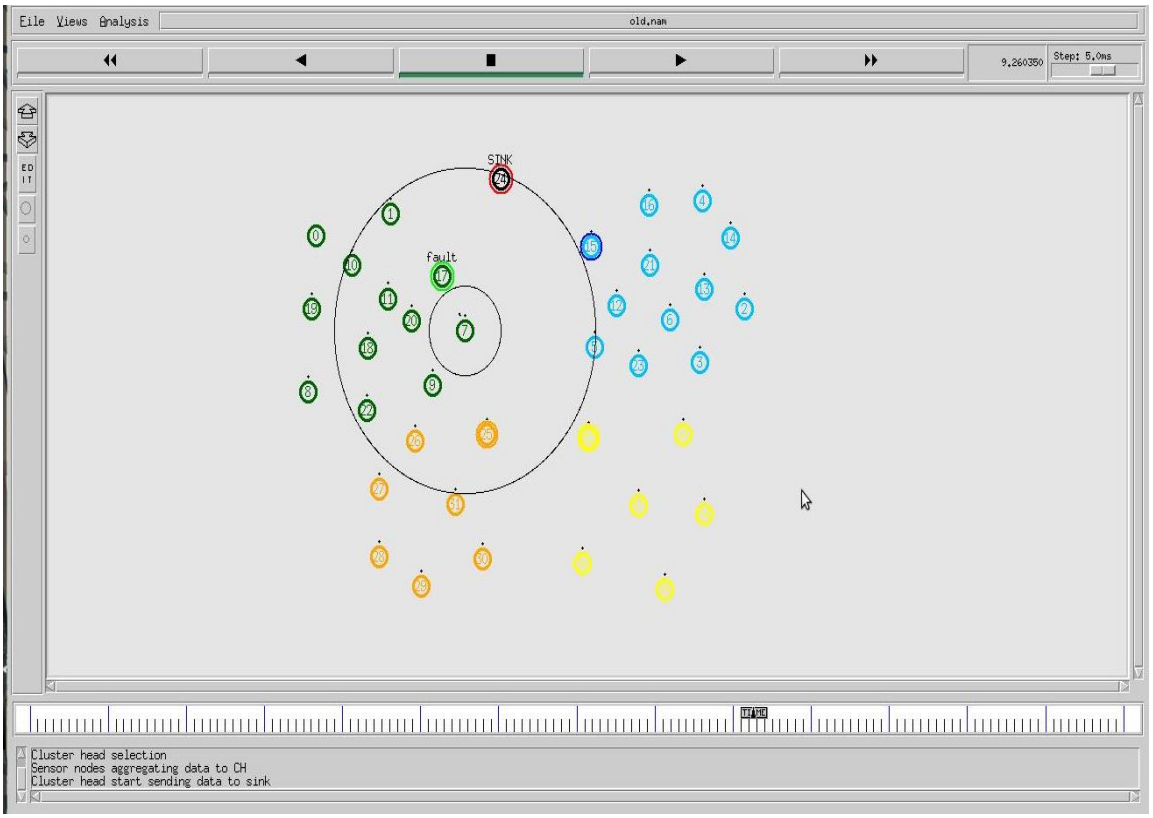


Figure 4.6 Data back-up node

As shown in te figure 4.6, the sensor network is deployed and whole network is divided into fix size clusters. The trust of each node is calculated on basis of number of packets re-transmitted and node which has maximum trust is selected as the node to maintain check points.

PROPOSED

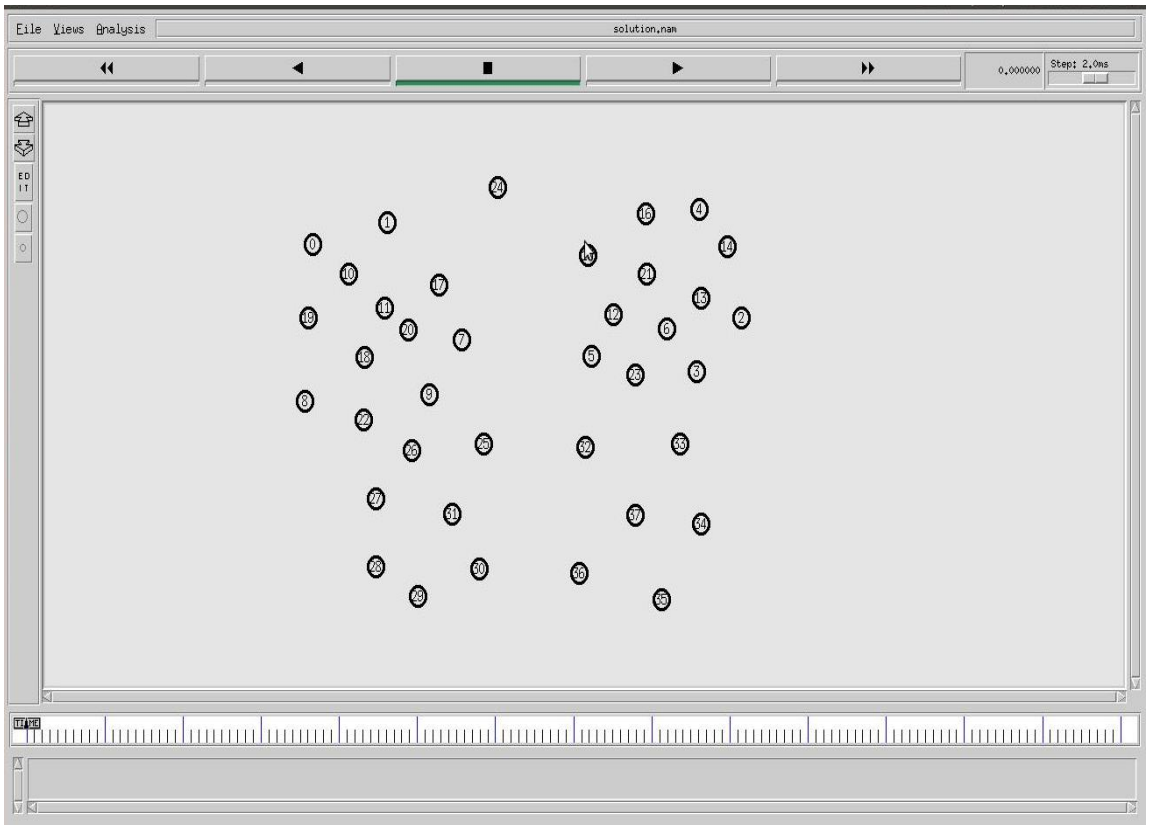


Figure 4.7 Deployment of sensor nodes

As shown in figure 4.7, The network is deployed with fixed number of sensor nodes and network as a whole is partitioned into fixed size clusters using location based clustering. The technique of LEACH protocol is applied to select cluster head in each cluster.

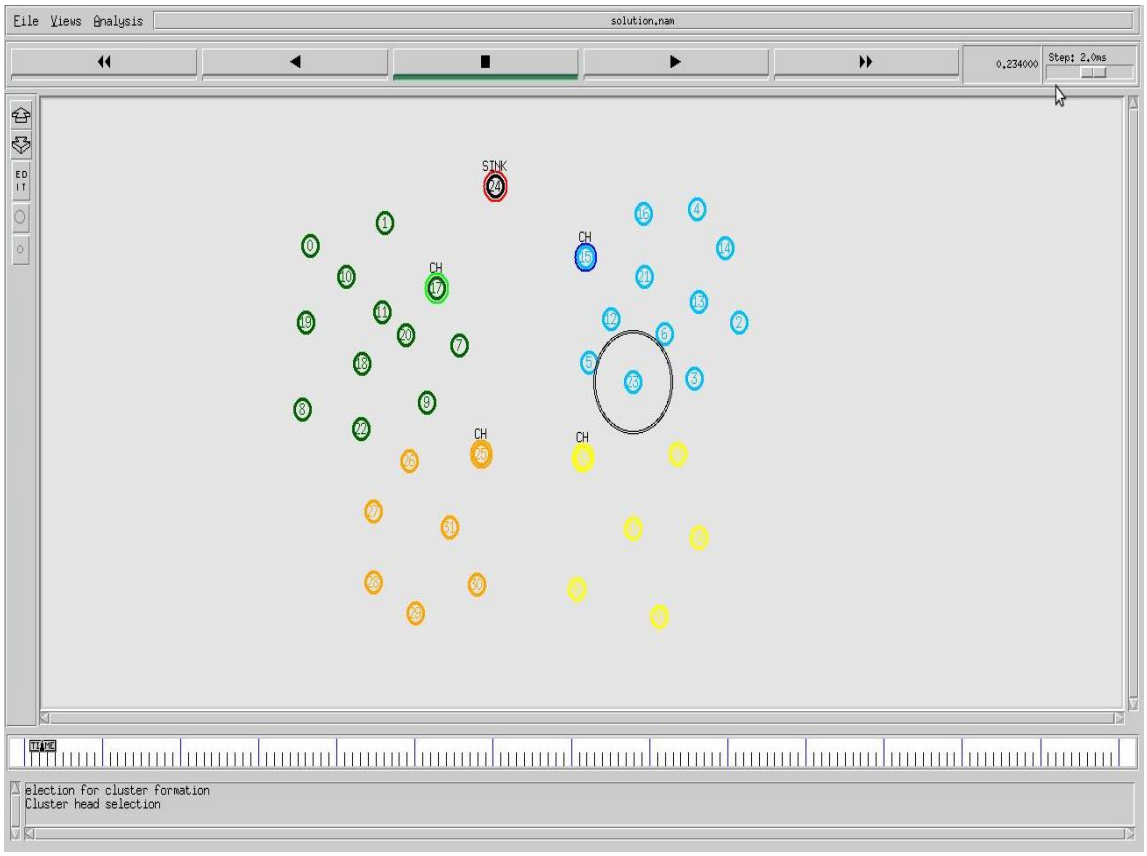


Figure 4.8 Nodes Deployment

As shown in figure 4.8, The network consists of n number of sensor nodes. Various clusters are formed and a cluster head is elected corresponding to each cluster.

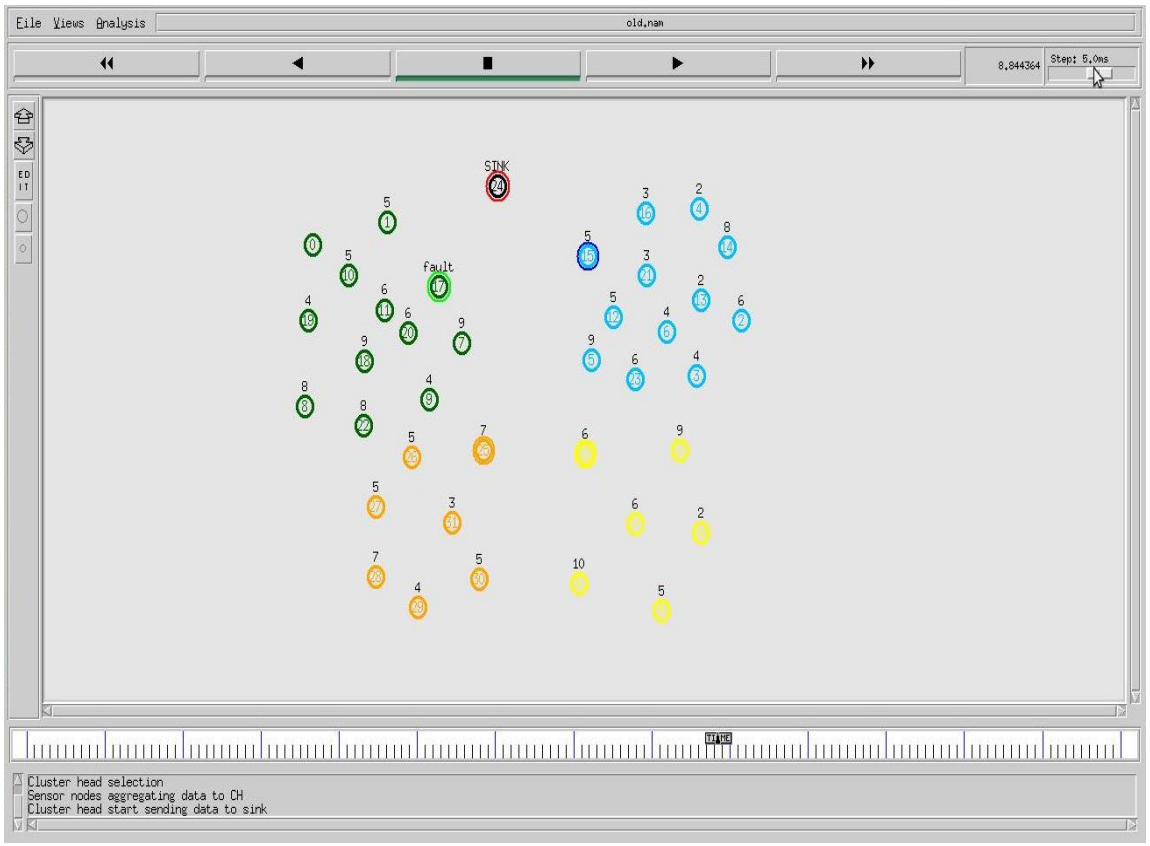


Figure 4.9 Trust Calculation

As shown in the figure 4.9, the trust of each node is calculated on the basis of number of packets re-transmitted in the network. The node which has maximum trust is selected as the best node to maintain the check points.

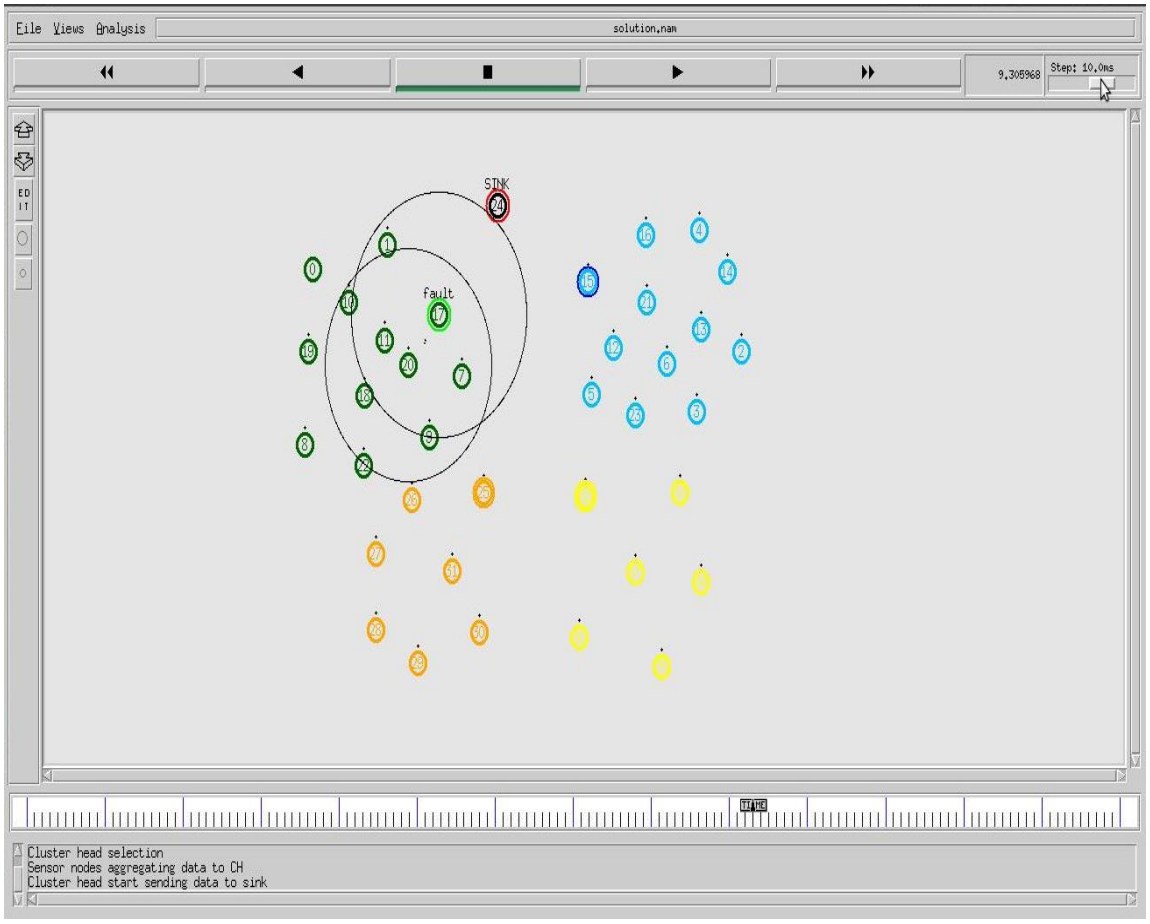


Figure 4.10 Selection of Back-up node

As shown in the figure 4.10, the overall network is partitioned into fixed size clusters and in each cluster, cluster heads are selected. The trust value and energy is calculated, node which has maximum energy and trust value is selected as the best node for the data backup.

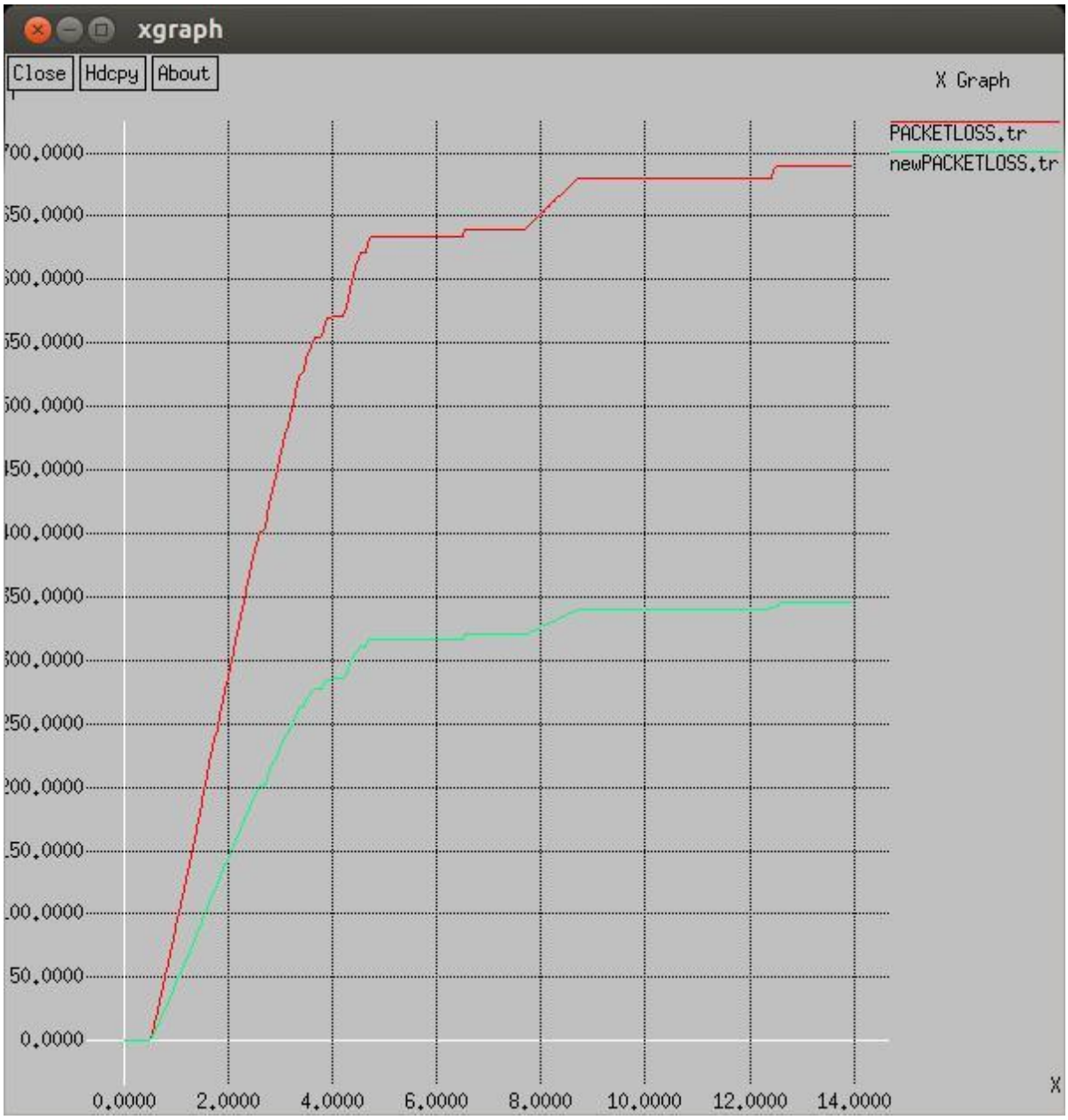


Figure 4.11 Packetloss Graph

As shown in the figure 4.11, the comparision of LEACH, Attack and proposed technique is shown in terms of delay. In is been analyzed that packetloss in the attack scenario is maximum and delay is reduced in proposed scenario due selection of most efficient back-up node.

Figure 4.12 Energy Graph

As shown in figure 4.12, the comparison of the proposed, LEACH and attack scenario is shown in terms of energy. It is been analyzed that energy consumption of the proposed scenario is least as compared to existing scenario.

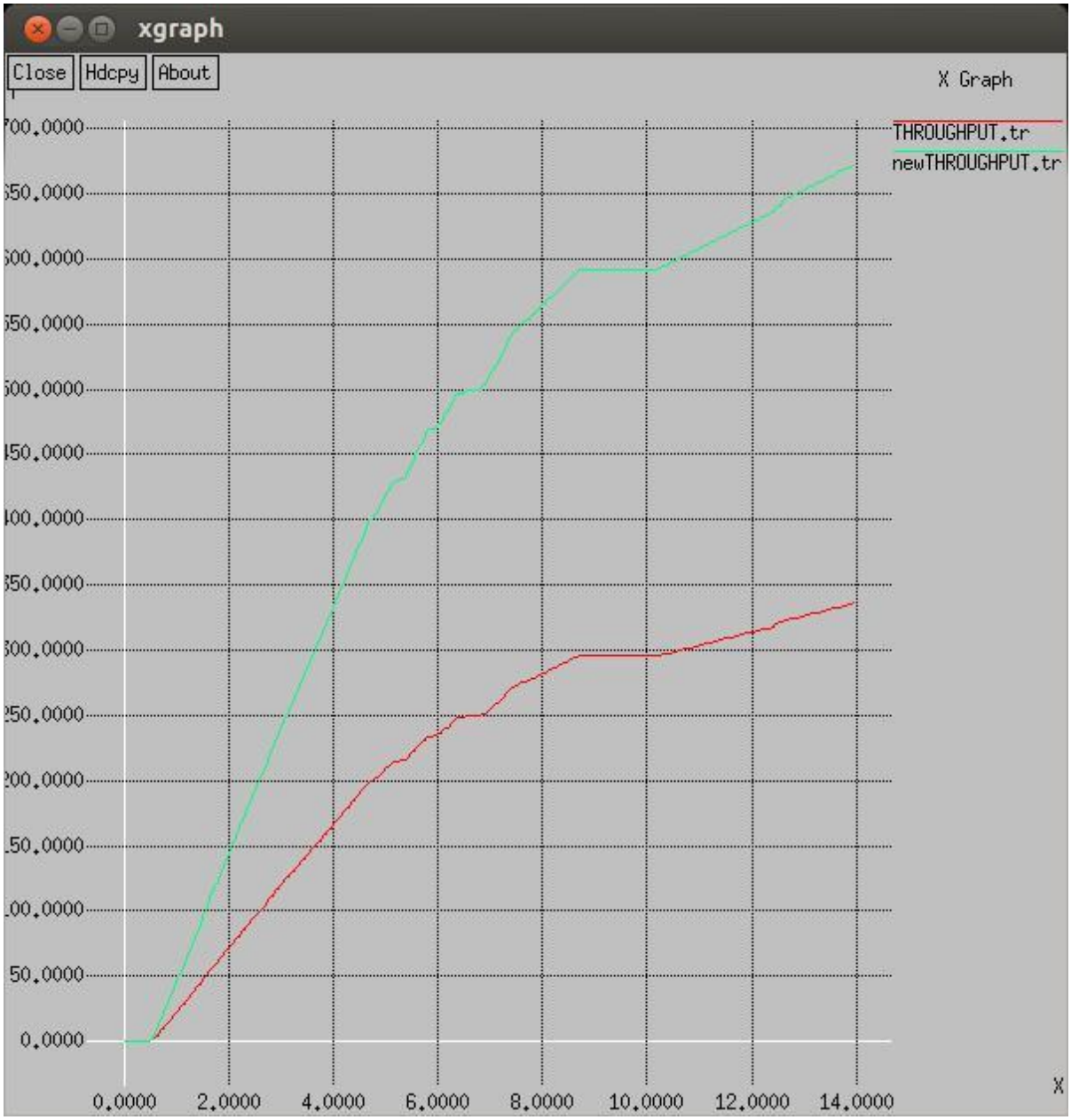


Figure 4.13 Throughput Graph

As shown in figure 4.13, the comparison of leach, attack and proposed scenario is shown in terms of throughput. It is been analyzed that throughput of the proposed scenario is maximum as compared to other two scenarios.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

The wireless sensor networks is the type of network in which sensor nodes sense the information and pass sensed information to base station. To increase lifetime of the sensor networks, cluster technique is widely used in which LEACH protocol performs well in terms of various parameters. In this work, technique of fault detection will be proposed which is implemented in NS2 and it is been analyzed that energy efficiency is improved by choosing the the most suitable backup node.

In this report, node failure prevention is accomplished using LEACH protocol and Check Pointing. These approaches are clubbed together to discover the suitable path for data packet transmission without losing much energy. The proposed technique looks for the nearest node in the cluster whose energy level is high and also has more the value of trust. The failure node is replaced with the node whose energy level and trust level is good and greater. This is accomplished with the help of check pointing. The link is generated even after the node replacement without affecting the transmission of packets. Thus this results in a Reliable, and energy-efficient communication over the network.

REFERENCES

[1]S. Rajasegarar, C. Leckie, and M. Palaniswami, “Anomaly detection in wireless sensor networks,” *IEEE Wirel. Commun.*, vol. 15, no. 4, pp. 34–40, 2008.

[2]Z. Wang, Q. Wen, Y. Sun, and H. Zhang, “A Fault Detection Scheme Based on Self-Clustering Nodes Sets for Wireless Sensor Networks,” *2012 IEEE 12th Int. Conf. Comput. Inf. Technol.*, pp. 921–925, 2012.

[3]S. Ameen and M. A. A, “Fault Tolerance Using Cluster in Wireless Sensor Network,” vol. 4, no. 4, pp. 351–356, 2014.

[4]C. A. Jerlin *et al.*, “Fault tolerance in wireless sensor networks,” *Int. J. Innov. Res. Adv. Eng.*, vol. 2, no. 2, pp. 142–146, 2015.

[5]E. U. Warriach, K. Tei, T. A. Nguyen, and M. Aiello, “Fault detection in wireless sensor networks,” *Proc. 11th Int. Conf. Inf. Process. Sens. Networks - IPSN ’12*, vol. 3, no. 3, p. 87, 2012.

[6]Alessandra De Paola, Giuseppe Lo Re, Fabrizio Milazzo, and Marco Ortolani, “QoS-Aware Fault Detection in Wireless Sensor Networks,” *Int. J. Dis. Sens. Networks*, vol. 2013, pp. 1–12, 2013.

[7]Manisha, Mr. Deepak Nandal, “Fault Detection In Wireless Sensor Networks,” *IPASJ Int. J. Comp. Sci.*, vol. 3, pp.6-10 , 2015.

[8]S. S. Singh, “Sensor Node Failure Detection using Check Point Recovery Algorithm,” pp. 3–6, 2016.

[9]Nikodem, M., & Wojciechowski, B. (2011, February). Upper Bounds on Network Lifetime for Clustered Wireless Sensor Networks. In New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on (pp. 1-6). IEEE.

[10] Pant, S., Chauhan, N., & Kumar, P. (2010). Effective cache based policies in wireless sensor networks: A survey. International Journal of Computer Applications (0975–8887) Volume, 11, 17-21.

[11] Gouvy, N., Hamouda, E., Mitton, N., & Zorbas, D. (2013, April). Energy efficient multi-flow routing in mobile Sensor Networks. In Wireless Communications and Networking Conference (WCNC), 2013 IEEE (pp. 1968-1973). IEEE

[12] Y. Jennifer, M. Biswanath and G. Dipak, (2008) “Wireless sensor network survey,”

Computer Networks, vol. 52, p. 2292–2330.
[13] Jiang, L., Bing Fang, & Li. (May, 2013) Energy optimized approach based on clustering routing protocol for wireless sensor networks. CCD Conference. IEEE
[14] Zhang, D., Li, G., Zheng, K., Ming, X., & Pan, Z. H. (2014). An Energy-Balanced Routing Method Based on Forward-Aware Factor for Wireless Sensor Networks. Industrial Informatics, IEEE Transactions on, 10(1), 766-773.
[15] B. Alakesh and G. R. Umapathi, (2014) "A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks: A Survey," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 2.
[16]Sharad N. Kumbharana1, Prof. Gopal M. Pandey (2013) "A Comparative Study of ACO, GA and SA for Solving Travelling Salesman Problem" International Journal of Societal Applications of Computer Science, vol. 2
[17] Somani, A. K., Kher, S., Speck, P., & Chen, J. (2006). Distributed dynamic clustering algorithm in uneven distributed wireless sensor network. Technical Reports [DCNL-ON-2006-005], Iowa State University
[18] Mamalis, B., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). Clustering in wireless sensor networks. RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, Y. Zhang, LT Yang, J. Chen, eds, 324-353
[19]Bakr, B. A., & Lilien, L. (2011, June). A quantitative comparison of energy consumption and WSN lifetime for LEACH and LEACH-SM. In Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on (pp. 182-191). IEEE
[20] Puccinelli, D & Haenggi.M.(2005).Sensor Networks: applications and challenges of ubiquitous sensing. IEEE circuits and systems magazine.5(3).(pp.19-31,2005).IEEE.
[21] Mendes, L. D., Rodrigues, J. J., Vasilakos, A. V., & Zhou, L. (2011, June). Lifetime analysis of a slotted ALOHA-based wireless sensor network using a cross-layer frame rate adaptation scheme. In Communications (ICC), 2011 IEEE International Conference on (pp. 1-5). IEEE
[22] Rai, M., K., D., (2013) "Dynamic Clustering in Wireless Sensor Network using Neural Network", International Journal for Advance Research in Engineering and Technology Vol. 1, Issue II , ISSN 2320-6802.

[23] S. Haidar, M. Mathieu and A. Hassan, (2014) “An energy efficient Genetic Algorithm based approach for sensor-to-sink binding in multi-sink wireless sensor networks,” Wireless Networks, vol. 20, p. 177–196.

[24] S. Rajasegarar *et al.*, “Distributed Anomaly Detection in Wireless Sensor Networks,” *Proc. 10th IEEE Int’l. Conf. Commun. Systems*, Singapore, Oct. 2006.

[25] Feilong Tang, Leonard Barolli, Jie Li ,”A joint design for distributive stable routing and channel assignment over multihop and multiflow mobile ad-hoc cognitive networks” vol. 8, no. 2, pp. 1–35, Mar./Apr. 2011.

[26] Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE “Mitigating Routing Misbehavior in Disruption Tolerant Networks” *publication year: 2012 vol:7 no 2, page(s):664-675*.

[27] ArjanDurresi, VamsiParuchuri and Leonard Barolli “Delay-Energy Aware Routing Protocol for Sensor and Actor Networks”*Publication Year: 2005 ,vol 1, Page(s): 292 – 298.*

[28] Myeong-Hyeon Lee, Yoon-Hwa Choi, “Fault detection of wireless sensor networks” 31 (2008) 3469–3475,Elseivier publications

[29] Chiara Buratti, Andrea Conti, Davide Dardari, and Roberto Verdone, “An Overview on Wireless Sensor Networks Technology and Evolution ” 6869-6896, Sensors 2009

[30] Holger Karl and Andreas Willig, “Protocols and Architectures for Wireless Sensor Networks ”, 2005 John Wiley & Sons, Ltd. ISBN: 0-470- 09510-5

Turnitin Originality Report

Report by Std Std

From Student (Plagiarism)

- Processed on 28-Apr-2017 09:47 IST
- ID: 806265344
- Word Count: 8981

Similarity Index
14%
Similarity by Source

Internet Sources:
4%
Publications:
13%
Student Papers:
N/A