Bhagwati Gaur al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 2, Issue 2, June 2015, pp. 272-277

Design & Implementation of Selfish Node Preventive Fault Handling Routing in WSN

Bhagwati Gaur[1], Seema Singh[2], Akhil Mahajan[3]

[1]Student, M. Tech, ICL-IET, Ambala
[2, 3] Assistant Professor, Dept. of ECE, ICL-IET,Ambala

***Abstract*- this paper presents selfish node preventive fault handling routing in wireless sensor networks. In this, it describes the attacks scenario with random sensor nodes. The objective is to handle these attacks & proposes a fault handling routing in network. Sensor nodes communicate with their neighbour nodes and hance energy will be consumed. The main issue is the energy wastage of unused nodes. So, to overcome this, it presents an optimization algorithm for reducing energy consumption. In this, optimal path selection is based on shortest distance between nodes which is to be calculated. The proposed mechanism is compared with energy aware clustering scheme and results shown to be better. The projected mechanism will be implemented with MATLAB.**

***Keywords* –Attacks in WSN, Wireless sensor networks, energy efficiency, MATLAB etc.**

I. INTRODUCTION

Wireless sensor network contains sensor nodes which are used to observe the surroundings, identify events of interest, manufacture data and work together in forwarding the data towards a sink, which could be a base station, storage node, or querying user. In this, some sensor nodes are deployed in unfriendly atmosphere for check the environment status and collection of surroundings data. When nodes are placed in this environment, it requires protection from outside but due to lack of facilities, sometimes it needs to be compromised. But it may cause some harmful attacks or some adversary effects for disrupt the network performance. The dropping packets and modifying packets are mainly two attacks i.e., nodes may drop or alter the packets that they are supposed to forward.

The main features of WSNs are limited memory, low power, energy constrained due to their small size. These sensor nodes are deployed in unfriendly atmosphere for check the environment status and collection of surroundings data. Though deployed in an unplanned manner they need to be self organized & self healing and can face steady reconfiguration [3].

Sensor nodes are the elementary components of any WSN and provide the following basic functionalities[6] 1) signal conditioning and data acquisition for different sensors;2)temporary storage of the acquired data; 3)data processing; 4)analysis of the processed data for diagnosis and, potentially, alert generation; 5)self- monitoring (e.g., supply voltage); 6)scheduling and execution of the management task; 7)management of the sensor node configuration; 8)reception transmission of forwarding data packets; 9)coordination and management of communication and networking.

The use of wireless sensor networks is increasing day by day and at the same time it faces the problem of energy constraints in terms of limited battery lifetime. As each node depends on energy for its activities, this has become a major issue in wireless sensor networks. The failure of one node can interrupt the entire system or application. Every sensing node can be in active (for receiving and transmission activities), idle and sleep modes. In active mode nodes consume energy when receiving or transmitting data. In idle mode, the nodes consume almost the same amount of energy as in active mode, while in sleep mode, the nodes shutdown the radio to save the energy

In WSNs the only source of life for the nodes is the battery. Communicating with other nodes or sensing activities consumes a lot of energy in processing the data and transmitting the collected data to the sink. In many cases (e.g. surveillance applications), it is undesirable to replace the batteries that are depleted or drained of energy. Many researchers are therefore trying to find power-aware protocols for wireless sensor networks in order to overcome such energy efficiency problems.

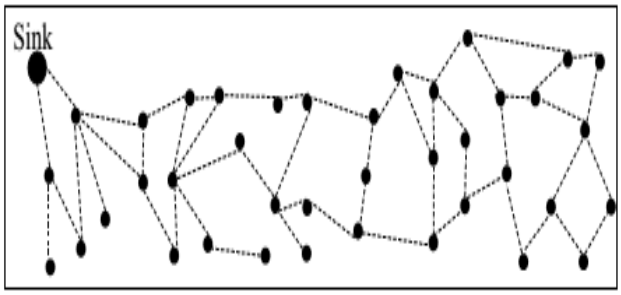

Figure 1: Wireless Sensor Network Schematic [1]

One reason behind the growing popularity of wireless sensors is that they can work in remote areas without manual intervention. All user needs to do is to fold the data sent by sensors, and with certain examination extract meaningful information from them. Usually sensor applications involve many sensors organized together. These sensors form a network and collaborate with each other to gather data and send it to the base station. The base station acts as the control centre where the data from the sensors are gathered for further analysis and treating. In a husk, a wireless sensor network is a system consisting of spatially dispersed nodes which use sensors to monitor physical or environmental circumstances. These nodes combine with routers and gateways to generate a WSN system [4].

The development of sensor networks requires technologies from three different research zones: sensing, communication, and computing (as well as hardware, software, and procedures). Thus, combined and separate progressions in each of these areas have driven investigation in sensor networks. Examples of early sensor networks comprise the

radar networks used in air traffic regulator. The national power grid, with its numerous sensors, can be viewed as one large sensor system. These systems were recognized with specialized computers and communication capabilities, and before the term "sensor networks" came into vogue [5].

Compared with existing schemes, our scheme has the following unique characteristics: (1) being effective in identifying both packet droppers and modifiers, (2) low overhead in terms of both communication and energy consumption

The rest of paper is ordered as follows. In section II, we discuss correlated work with wireless sensor networks. In Section III, It defines routing techniques. In Section IV, it describes proposed work of system. Finally, conclusion is explained in Section V.

II. LITERATURE REVIEW

In Literature, author studied the Existing Fault Recovery approaches for WSN vary in forms of architecture, protocols, detection algorithm and detection decision fusion algorithm. They Provided Energy Efficient and Fault Tolerant Routing LEACH which is a modified version of the well known LEACH Protocol. EF-LEACH provides vital solutions to some shortcomings of the pure LEACH .It provide network fault tolerant and achieves reliability and quality of service. Basically WSN faces resource constraints, high failure rates and fault caused by wireless channel and wireless sensor nodes. When a node gets failure it immediately applies its backup paths as the main path for data delivery of next incoming packets. This protocol reduces the number of dropped data packets and increases robustness of the entire network by maintaining the data packet transmission even in presence of faults [6].

Some authors proposed that topology control in a sensor network balances load on sensor nodes & increases network scalability and life time. It is envisioned that sensor nodes will be on the cubic millimetre scale, posing stringent constraints on the processing communication and storage capabilities of sensor nodes. While it is important to continue perusing novel algorithm and protocols to squeeze the most out of the existing design space, it is equally important to explore new design paradigms for future [7].

Some proposed routing algorithm (Resistance Distance Routing algorithm, RDR algorithm) which optimizes the routing path based on the theory of resistance distance in electricity. This paper describes the whole process of RDR algorithm in detail, and simulates it with MATLAB. Simulation results show that RDR algorithm is superior to the GEAR (Geographical and Energy Aware Routing) algorithm both in the efficiency of energy consuming and the sturdiness of the network [8].

Some proposed that to reduce power consumption utilizing duty cycling, sensor nodes switching to sleeping mode for most of the time is commonly used in WSN. However sensor nodes may not be able to stay awake simultaneously to communicate with each other.

Some presented a new protocol for routing taking the concept of swarm intelligence. In this, they provided many investigation schemes for routing protocols using different swarm intelligence. After this, they provided a comparison on the basis of energy efficiency, lifetime, fault detection, scalability, success rate etc. These swam based protocols can remove several problems like battery life, maintainability, survivability, adaptability etc. [10].

Some proposed an energy efficient protocol called Enhanced Energy Efficient Chain-based Routing Protocol in WSN. In this work, they minimized energy consumption and transmission delay. They organised these sensing nodes as horizontal chains & vertical chains. The Head was selected on the basis of remaining energy of nodes and distance from head of upper level. In this scheme, each sensing node transmitted its data to its head. The simulation results showed that EECRP outperforms PEGASIS, ECCP and EECRP in terms of network lifetime, energy consumption [11].

Author presented some general data forwarding algorithm that can be set so that delay can be minimized. To provide a solution, each node provided a route to sink node. The main metric used for this problem is based on the end-to-end total cost objective. The starting node that forwards the data is uncertain about its no. of relays, their wake up time and rewards but only knew about probability distribution of these quantities. [12].

III. FAULT TOLERANCE IN WSN

The sensor nodes may be deployed in harsh or hostile environments leaving the nodes potentially vulnerable to environmentally induced failure or attack. As a result, sensor nodes may be easily damaged or depleted of energy altering the network topology and fragmenting routing paths. This dynamic characteristic of the network is especially critical to routing protocols where energy is lost in transmitting along failed routing paths. As noted above, sensor nodes are not readily replaced or recharged and hence the networks and employed protocols must complete their objectives in the presence of one or more failed nodes. This clearly establishes the value of employing mechanisms and protocols that persist correctly after the onset of network failures. This characteristic is referred to as fault-tolerance.

Fault-tolerance is the quality or ability of a functional unit to perform a required task in the presence of some number of faults. Fault-tolerance is applied to increase the reliability of a system. Some expand the domain of the topic to dependability which encompasses availability, reliability, safety, integrity, and maintainability [4]. In this discussion, availability is the readiness of a system to provide a service. Reliability is "continuity of correct service" [4] or the probability of survival, both of which coincide with the previous definition for reliability.

A. Sources of Faults

At least two components of a sensor node, sensors and actuators, will directly interact with the environment and will be subject to a variety of physical, chemical, and biological forces. Therefore, they will have significantly lower intrinsic reliability than integrated circuits in fully enclosed packaging. In enterprise scenarios it becomes highly important to hide the details of the underlying sensor networks from the applications and to guarantee a minimum level of reliability of the system. One of the challenges faced to achieve this level of reliability is to overcome the failures frequently faced by sensor networks due to their tight integration with the environment.

Failures can generate false information, which may trigger incorrect business processes, resulting in additional costs.

Sensor networks are inherently fault prone due to the shared wireless communication medium: message losses and corruption (due to fading, collision and hidden node effect) are the norm rather than exception. Moreover, node failures (due to crash and energy exhaustion) are the commonplace. They are also prone to failure due to hardware failure, communication link errors, malicious attack, and so on. Thus, sensor nodes can lose synchrony and their programs can reach arbitrary states. Since on-site maintenance is not feasible, sensor network applications should be local and communication-efficient self-healing.

Maintenance of continuous connectivity in a wireless sensor network after it is deployed in a hostile environment is also a major issue. Constrained by the low user to node ratio, limited energy and bandwidth resources, entities that are usually mobile, networks without fixed infrastructure and frequent failure due to problems of energy, vulnerability to attack etc, a need for wireless sensor networks to be self-organizing and self-configuring so as to improve performance, increase energy efficiency, save resources and reduce data transmission arises. Also, a WSN is prone to several types of faults, such as crash fault, transient fault, byzantine fault etc that affect the normal functioning of the WSN system. Thus, fault tolerance is a major issue confronting the development of highly scalable distributed WSN.

B. The Need for Fault Tolerant Protocols

Sensor networks distribute general collapse issues (such as node and link failure) with conventional wired and wireless networks, in addition to introduce new fault sources (such as multi-node failures). In these Fault tolerant techniques, it includes various tools that have become engineering standard such as SNMP and TCP/IP, in addition to more dedicated and more proficient techniques that have been comprehensively researched. The faults in sensor networks cannot be approached in the same way as in conventional wired or wireless networks due to the following reasons:

- Conventional network protocols are usually not anxious with energy expenditure, since wired networks are constantly powered and wireless ad hoc devices can get recharged frequently;
- traditional network protocols aim to attain point-to-point consistency, whereas wireless sensor networks are concerned with dependable event discovery;
- in sensor networks, node failures occur much more often than in wired, where servers, routers and client machines are supposed to work generally most of the time; this implies that closer monitoring of node health without incurring important overhead is needed;
- traditional wireless network protocols based on functional MAC layer protocols that stay away from packet collisions, hidden terminal problem and channel errors by using physical carrier sense (RTS/CTS) and virtual carrier sense (monitoring the channel).

IV. PROPOSED FAULT TOLERANCE SCHEME IN WSN

Fault detection is the first stage of fault management, where an unpredicted failure should be correctly recognized by the network system. The failure detection approaches in WSNs can be classified into two types: centralized and distributed approach.

Centralized approach is an ordinary solution to recognize and localize the cause of failures or suspicious nodes in WSNs. Usually, a physically or logically centralized sensor node takes duty for monitoring and tracing failed or misbehaviour nodes in the network. Most these approaches consider the central node has unlimited resources (e.g. energy) and is able to execute a wide range of fault management maintenance. They also believe the network lifetime can be extended if complex management work and message transmission can be shifted onto the central node. The central node normally adopts an active detection model to retrieve states of the network performance and individual sensor nodes by periodically injecting requests (or queries) into the network. It analyzes this information to identify and localize the failed or suspicious nodes.

Distributed approach encourages the concept of local decision-making, which evenly distributes fault management into the network. The goal of it is to allow a node to make certain levels of decision before communicating with the central node. It believes the more decision a sensor can make, the less information needs to be delivered to the central node. In the other word, the control centre should not be informed unless there is really a fault occurred in the network.

A. Attacks in Network

Misdirection attack can be performed in different ways: Packets forwarded to a node close to the actual destination. This kind of misdirection attack is less intense, because packets reach to the destination but from a different route which further produces long delay thus decreasing throughput of network. Packets forwarded to a node at a large distance from the actual destination.

Malicious nodes act as a black hole to attract all the traffic in the sensor network. Attackers listen to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Inserts itself between the communicating nodes it is able to do anything with the packets passing between them.

It uses Hello packets as a weapon to convince the sensors in WSN. Attackers with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes. Sensors are thus persuaded that the adversary in their neighbour. Victim nodes try to go through the attacker.

Attacker records the packets or bits at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Attack does not require comprising a sensor in the network rather it could be performed even at the initial.

Failure detection via neighbour coordination is another example of fault management distribution. Nodes coordinate with their neighbours to detect and identify the network faults (i.e. suspicious node or abnormal sensor readings) before consulting with the central node. For example, in a decentralized fault diagnosis system, a sensor node can execute a localized diagnosis algorithm in steps to identify the causes of a fault. In addition, a node can also query diagnostic information from its neighbours (in one-hop communication range). This allows the decentralized diagnostic framework to scale easily to much larger and denser sensor networks if required.

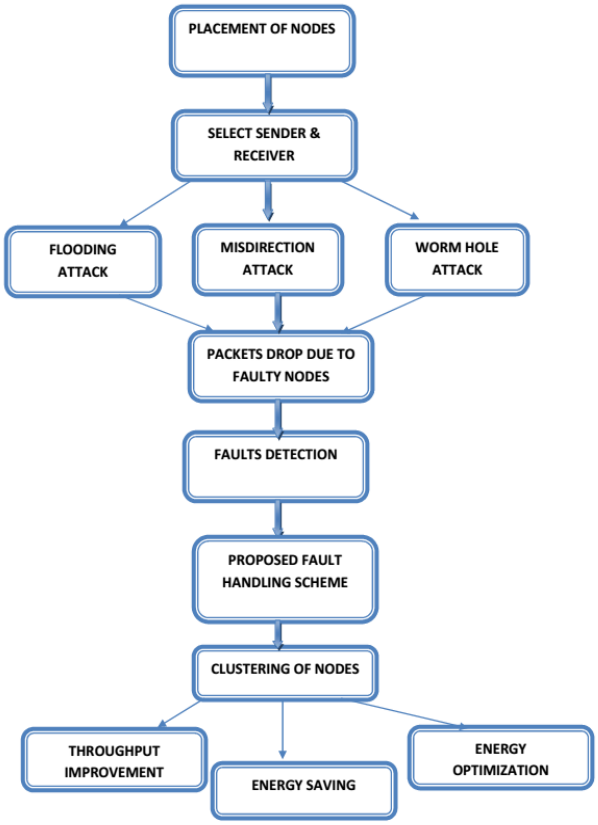

Figure 2: Proposed System Model

To evaluate the performance of the proposed approach, we have used the following metrics:

- Recovery delay: these metric measures the time it takes to find and establish an alternative route to the sink in case of failure of the path in use. We assume that the damage did not cause any partitioning and thus an alternative path is available. Note that this delay does not involve any movement.
- Total number of messages sent by the sensors: This is to assess the message overhead of the partition detection algorithm on sensors.
- Lifetime: Critical to any wireless sensor network deployment is the expected lifetime. The goal of both the environmental monitoring and security application scenarios is to have nodes placed out in the field, unattended, for months or years. The primary limiting factor for the lifetime of a sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize total network lifetime. In many deployments it is not the average node lifetime that is important, but rather the minimum node lifetime.

V. RESULTS & DISCUSSION

Following are the implementation results for the scenario. In this work, take the scenario for 50 nodes and following result will show the information about the placement of sensor nodes in an area. The simulation environment is to randomly distribute 50 sensor nodes to an 100m*100m square. The initial energy of each node is provided. In each round, the sensor node will deliver a packet. All sensor nodes are stationary and homogenous. All sensor nodes can adjust their power levels based on distance.

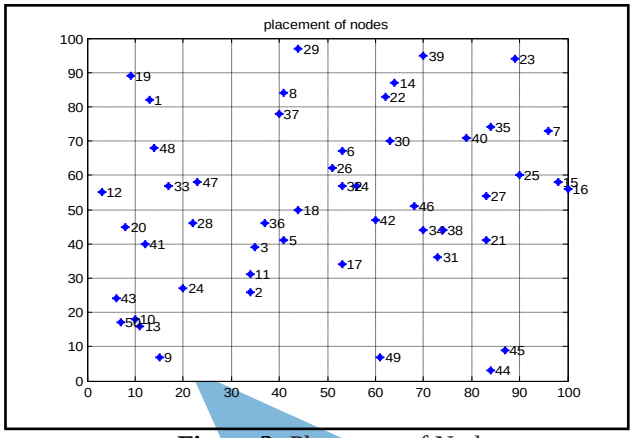

Figure 3: Placement of Nodes

We suppose that all sensor nodes have the same capability in term of processing, communication and power supply etc. It is practical for each sensor to adjust its power level. After the deployment of the sensor nodes, there is a Head node selection by polling method. In a heterogeneous sensor network, the basic sensors are simple and perform the sensing task, while some other nodes, often called the heads, are more powerful and focus on communications and computations.

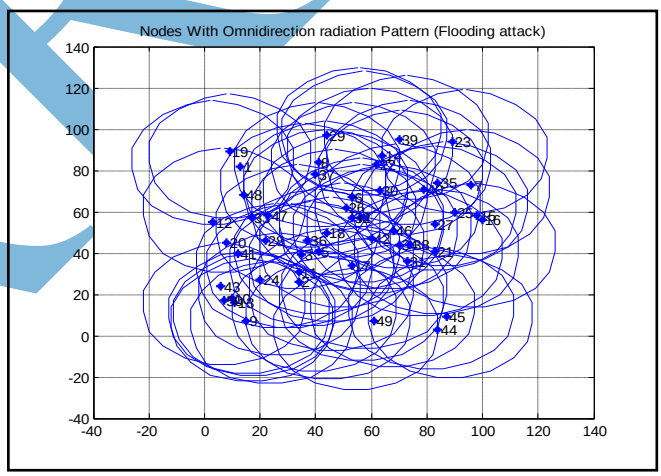

Figure 4: Flooding Attack on Network

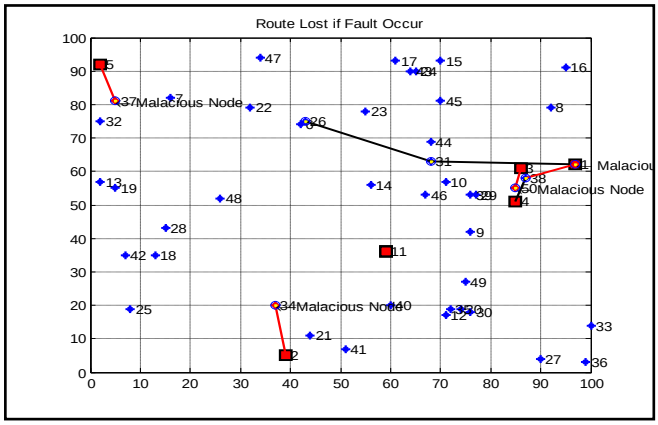

Figure 5: Fault Nodes Detection

In proposed routing scheme, first, the source node will determine whether to use direct transmission or multi-hop transmission based on the determination criterion If the distance d is less, it will choose direct transmission which is

more energy efficient. If d is greater than threshold, it will choose multi-hop transmission. It is worth noting that d is a theoretical value of the threshold distance and sometimes direct transmission is also more energy efficient than multi-hop transmission After determination of the sub-optimal hop number opt n , the source node will choose a set of its neighbours with distance d as candidates of its next hop. Finally, the neighbour node which is closest to the sink node will be chosen as the next hop. Thus, more energy is caused therein. Second, we next hop should be the closest one to sink node. In other word, progress should be made toward sink node during each hop routing.

When the next hop node is chosen, the source node will send a short RREQ (Route Request) message to the next hop directly through unicast. Once the neighbour node receives this RREQ message, it will send an ACK (acknowledge) message to its previous (source) node. Then, it will add its own location information into the RREQ message and send it to its next hop neighbour in an iterative manner like its previous node. Finally, the RREQ message will reach sink node with complete route information inside the RREQ message and a RREP (Route Reply) message will be sent back in a reverse way by sink node to the source node based on the assumption of symmetric link.

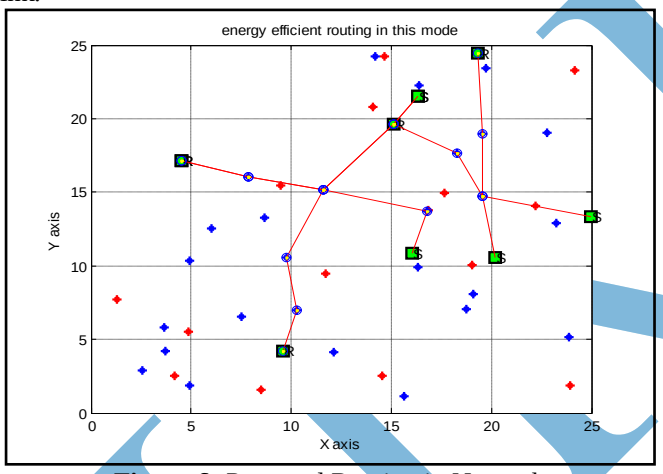

Figure 6: Proposed Routing in Network

In this, it uses the clustering approach for saving the energy. In this, firstly it detects the faults under clustering using energy aware technique. But in this, there is loss of energy. So, it requires energy optimization.

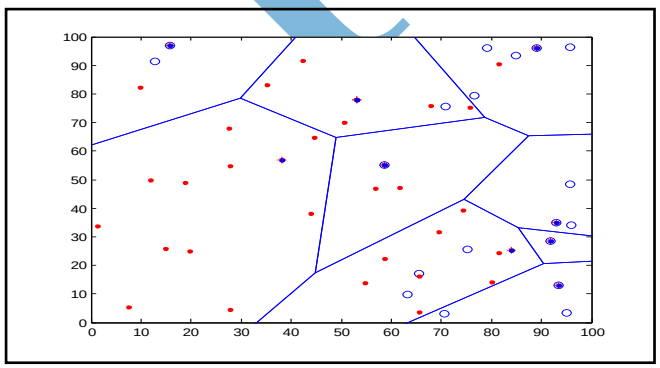

Figure 7: Energy Aware Clustering Approach in Network

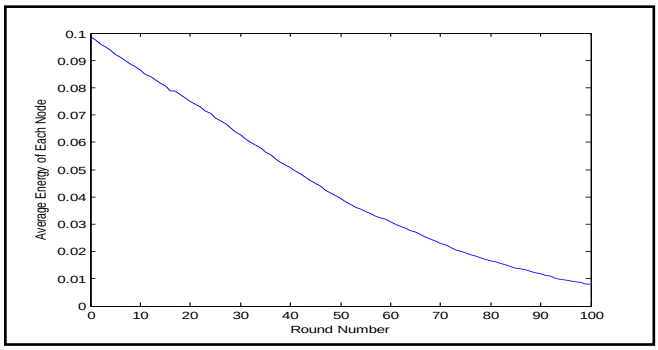

Figure 8: Average Energy Response using Energy Aware Approach

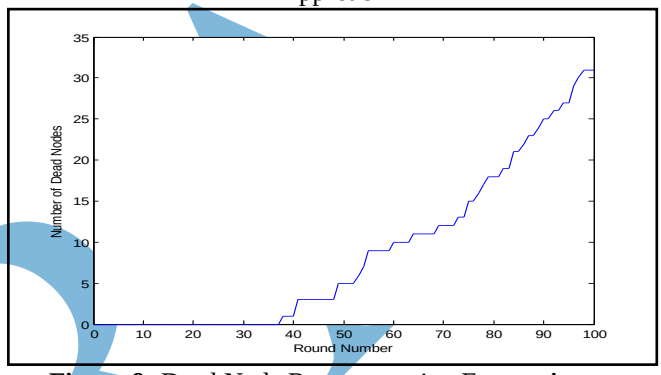

Figure 9: Dead Node Response using Energy Aware Approach

To overcome the problem of dead nodes, it requires optimization of energy using energy efficient approach under clustering.

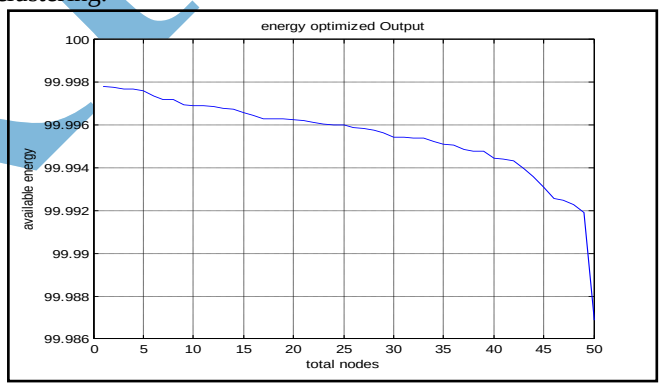

Figure 10: Optimized Energy Response using Proposed Approach

VI. CONCLUSION

In this work, it presents selfish node preventive fault handling routing in wireless sensor networks. In this, it describes the attacks scenario with random sensor nodes. The objective is to handle these attacks & proposes a fault handling routing in network. Sensor nodes communicate with their neighbour nodes and hance energy will be consumed. The main issue is the energy wastage of unused nodes. So, to overcome this, it presents an optimization algorithm for reducing energy consumption. In this, optimal path selection is based on shortest distance between nodes which is to be calculated. It also presents energy optimization scheme under clustering of nodes. The main attacks covered here are misdirection attack, wormhole attack and flooding attack etc. In this, it basically defines the way of handling the faults or various attacks in

network. And also provides the way for energy efficiency in system.

REFFERENCES

[1] S. Ozdemira, Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview", 2009.

[2] L.T Nguyen, X.Defago, R.Beuran, Y.Shinoda, "An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks", 2008.

[3] W.H Liao, H-H Wang, "An asynchronous MAC protocol for wireless sensor networks", 28 July 2008.

[4] J. Zhua, K.L Hunga, B. Bensaoua, F.N Abdesselam, "Rate-lifetime tradeoff for reliable communication in wireless sensor networks", 29 September 2007.

[5] H. Shih, J. Ho, B. Liao, "Fault Node Recovery Algorithm for a Wireless Sensor Network" IEEE Sensors Journal, Vol. 13, No. 7, 2013.

[6] M. Masdari and M. Tanabi, "Multipath Routing protocols in Wireless Sensor Networks: A Survey and Analysis", International Journal of Future Generation Communication and Networking Vol.6, No.6, 2013.

[7] M. Sharawi, I.A Saroit, H. Mahdy, E. Emary, "Routing Wireless Sensor Networks Based On Soft Computing Paradigms: Survey", International Journal on Soft Computing, Artificial Intelligence and Applications (IJSCAI), Vol.2, No.4, 2013.

[8] S. Sharma, Dr. P. Mittal, "Wireless Sensor Networks: Architecture, Protocols", Volume 3, Issue 1, 2013.

[9] E.P.K Gilbert, B. Kaliaperumal and E.B singh, "Research Issues in Wireless Sensor Network Applications: A Survey",International Journal of Information and Electronics Engineering, Vol. 2, No. 5, 2012.

[10] Ms. P. Tyagi, Ms. S. Jain, "Comparative Study of Routing Protocols in Wireless Sensor Network", Volume 2, Issue 9, 2012.

[11] O.D Incel, "A survey on multi-channel communication in wireless sensor networks", 2011.

[12] L.D.P. Mendes, J.J.P.C. Rodrigues, "A survey on cross-layer solutions for wireless sensor networks", 2011.

[13] C.Tana, J.Zoua, M. Wanga, R. Zhang, "Network lifetime optimization for wireless video sensor networks with network coding/ARQ hybrid adaptive error-control scheme", 2011.

[14] M.A Yigitel, O.D Incel, C.Ersoy, "QoS-aware MAC protocols for wireless sensor networks: A survey",2011.

[15] L. Almazaydeh, E. Abdelfattah, M. Al- Bzoor, and A. Al- Rahayfeh, "Performance Evaluation Of Routing Protocols In Wireless Sensor Networks", International Journal of Computer Science and Information Technology, Volume 2, Number 2, 2010.

