BPR: An Efficient Technique to by-pass the Infected Areas in WSN

Nanditha.T .K
MTech
Siddaganga Institute of Technology
Tumakuru, Karnataka, India

Shreenath. K .N
Associate Professor
Siddaganga Institute of Technology
Tumakuru, Karnataka, India

***Abstract* - Wireless Sensor Network is one among the recent technology and most widely used. A wireless sensor network is delineated as set of small sensor node. These sensor nodes co-ordinates to perform some specific task. When these sensor nodes are attacked or corrupted, it leads to various issues like hardware failures and software failures. The issues of infected nodes will disturb the normal communication of the network and also affects the generated data and incoming data. The inaccurate data from the affected nodes leads to wrong decision making, communication disruption and misleading packet translation. These problems of the affected node are threat to the quality of service requirements. The data from the other nodes may also get stuck in these affected or infected nodes which lead to packet loss. Even though several existing methods like (Bound Hole and GAR) can be used to avoid these problems, but their performance is limited to some limitations like unnecessary transmission and routing loops. The solution to these problems is to take the different route i.e. to bypass the infected node or area using twin rolling ball technique and to divert the packets that are caught inside that particular infected area.In this BPR technique Twin Rolling ball mechanism is employed. This mechanism is used to find the next hop from the local minima node and to forward the packets out of the infected nodes. The STL mechanism is used to identify the infected nodes.**

Keywords:* *Wireless Sensor Networks, Routing loops, Quality of Service,Twin Rolling Ball, STL, GAR, Bound Hole .

I. INTRODUCTION:

Everything in the world depends on technology. Wireless sensor network technology is one among them .It has got good feedback and high adoptions from various levels of application. WSN provides a bridge between the virtual and real physical world and has the ability to observe the previously unobservable situation at a fine resolution over large scale [1].WSN is collection of sensors which are capable of sensing, computing and communicate.

Sensor network extend the present internet deep into the physical setting.Information collected and transmitted on a sensor network describes the conditions of physical surroundings for instances like temperature, humidity, or vibration etc. [2].WSN has many applications and it is most widely used in various remote event monitoring applications, we concentrating on the issues in hazardous areas and hostile ambiance.

In a typical sensor network, each sensor node has microprocessor and a memory (small) for processing and task scheduling. Each sensor also equipped with the one or more sensing devices. Each sensor node communicates to its neighbour nodes wirelessly within the radio communication range.

A key part of sensor network is the networking.Networking permits the geographical distribution of the sensing nodes and their placement nearer to the signal sources. In the sensor network all the nodes utilises the radio links for communication. Each node talks directly only to its immediate neighbours within the radio range. In every network we assume that node knows their geographic position so to transfer the data or some information from source node we need to find the best path to reach the destination or sink. The procedure of selecting best path among many paths is called Routing.
Two classes of routing in WSN are *Geographic routing and Routing based on virtual co-ordinates*. Here, we consider geographic routing. Geographic routing depends on the physical location information of each node which can be obtained with the help of *GPS*. The best known method for this kind of routing is **greedy forwarding.** With regard to the greedy forwarding knowledge data packets are sent to the neighbour node which is nearer to destination node than the current node.GF is based on the shortest path procedure which causes the situation known as Local minima problem [1].Local minima is that the scenario once a packet gets stuck at a node whose 1-hop neighbours are all farther off from the destination node and the situation oflocal minima is solved with the help of our technique BPR i.e. By-pass Routing.

Due to the restricted capability of sensor nodes, nodes suspect to fail. Due to the incapability of sensor node the sensing and communication of the network gets affected. This may leads to the malware attacks, hardware failures and software corruption which sequentially affect the network applications. So, to avoid the packet loss during these situations we need to find the fast and alternative routes to send the packets to its intended destination. This can be achieved by avoiding the infected area i.e. the node which fails to perform the normal operation or which malfunctions is considered as infected node and the surrounding area is calledinfected area. The infected node and the infected area are identified by the Stop Transmit and Listen method. This paper provides the solution to the 2 situations i.e. local minima problem and to bypass them.Hence By-pass routing technique.

II. LITERATURE SURVEY:

The research communities of WSN are concerned about few issues including fault resilience, network lifetime and localisation, mobility of sink nodes, security, and routing. *Routing* receives more interest among other issues. Most of the protocols evolved for sensor network useGreedy Forwarding (GF) methodology. GF forwards a packet to the sink node or destination node with through its one-hop neighbours [4] .The current node that receives the packet repeat the methodology till the packet reaches its destination. This procedure has proved the minimum consumption of energy and does not require additional routing overhead. But, it experience the local minima problem or holes problem [3] .*Local minima* is the issue of the geographic routing which is caused by the “holes” or node failure that blocks the greedy forwarding process. It refers to the situation where there exists no other neighbour node that has the less distance to the destination than the current node and hence packet cannot be forwarded further and gets stuck.

So, to get the stuck packets from the local minima node and forward the packets to the particular destination many methods were proposed and suggested.

P.Bose, Morin, I.stojmenovic and J.urrutia in “Routing with guaranteed delivery in Ad-hoc wireless networks “, proposed an idea of combining the greedy forwarding and the perimeter routing on a planar graph that represents the same connectivity as the original network. If a path exists, they showed the guaranteed delivery, but perimeter routing requires the planar graph maintenance which is more expensive [5].

Karp and Kung proposed Greedy perimeter stateless routing for wireless networks. From the simulations using GPSR protocol most of the packets reach their destination by greedy forwarding only. Therefore keeping planar graph at all the nodes is unnecessary. But, it failed for the local minima problem most of the time [6].

Qing Fang, Jie Gao, Leonidas J.guibas , Proposed BOUNDHOLE algorithm to solve the local minima problem .This mechanism try to identify the local minima node and a route is constructed around the hole, which consists of all the stuck nodes. The boundary nodes has to hold the boundary message .But in this mechanism there is more possibility of finding the false boundary and it has possibility of falling into the routing loop. Boundary nodes also need to retain the shape of the holes that in turn requires extra memory [7].

Wen-Jiunn Liu, Kai-Ten Feng in Greedy routing with anti-void Traversal for wireless sensor networks proposed GAR mechanism to tackle the issues of the Bound Hole. It employs the rolling ball method at the local minima node to find the next hop. Though it is more efficient than the Bound Hole, it visits the unnecessary nodes, resulting in more energy consumption [8].

Disadvantages of the existing system:

- More probability of leading into the loops and packet loss
- Visiting the unnecessary nodes.
- High energy consumption.
- Extra memory usage.

The proposed technique in this paper is similar to rolling ball technique used in GAR.The detail description of the BPR is explained in the further sections.

Objectives:

- To find the solution to get the stuck packets out of the local minima node.
- To compose a technique that can by-pass the infected areas and infected nodes.
- To switch the direction of the incoming traffic to the unaffected regions.

III. PROPOSED SYSTEM

3.1 Assumptions:

- Network consists of nodes within 2-dimensional Euclidean plane
- Nodes are randomly scattered in the region and assuming all the nodes are homogeneous.
- Location of the destination node is known in prior by the source node.
- Location of other nodes in set is known using frequent updates.

3.2Identification of the infected nodes and infected areas:

A simple and effective scheme proposed to identify the infected or malicious node is Stop Transmit and listen method (STL) [9].Each node in sensor network will have built-in time limit to conclude their transmission. Each node is having the capability of finding malicious node.Nodes in the network will sense the data and send to the sink node. For every few seconds each node stops their transmission and listens for malicious behaviour. The malicious nodes or attacker nodes are not aware of the non-transmitting time of the nodes in network. When the malicious node transmits the data or try receiving in the non-transmitting time then those nodes are considered as the infected nodes. The malicious behaviour is broadcasted in the network and hence neighbour nodes come to know about all the nodes which are infected.

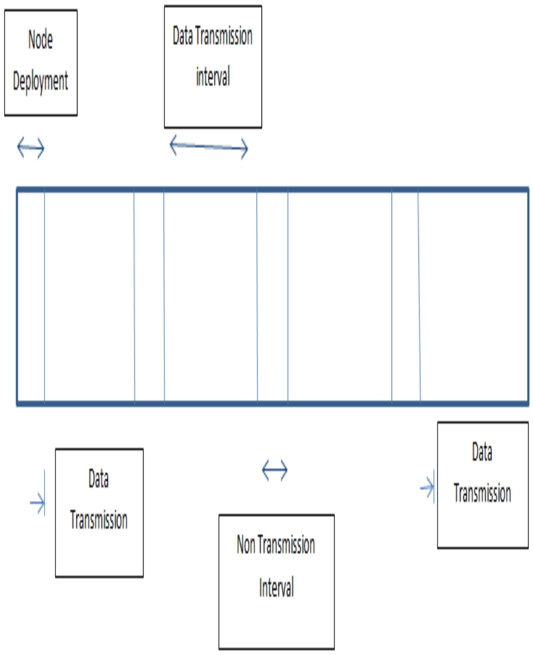

Figure 2: STL operation

STL mechanism has three stages:

1. Data Transfer
2. Stop and Listen
3. Removal of malicious nodes.

*3.2.1. Data Transfer:*Once the nodes are distributed over the region, each node will be having the built-in time limit to conclude their transmission.The proposed STL scheme doesn’t require any type of network topology for data transmission. The sensed data is forwarded to the sink node as shown in *figure 1*.

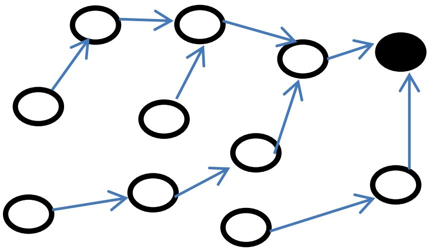

Figure 1: Data transfer

*3.2.2. Stop and Listen:*For every few seconds nodes in the network stop their transmission in STL scheme. The operation of STL is shown in *figure 2*.

The malicious node does not know about the non-transmission time allocation in sensor nodes. So, malicious nodes may try to send or receive the data in non-transmitting time interval. The malicious node behaviour of the node is listened by the neighbour nodes in non-transmitting time interval as shown in *figure 3*.

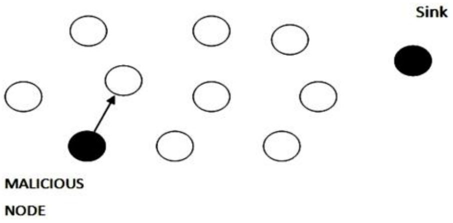

Figure 3: Non-transmitting interval

3.2.3. Removal of malicious nodes: The malicious behaviour of the node is broadcasted throughout the network as shown in *figure 4*.

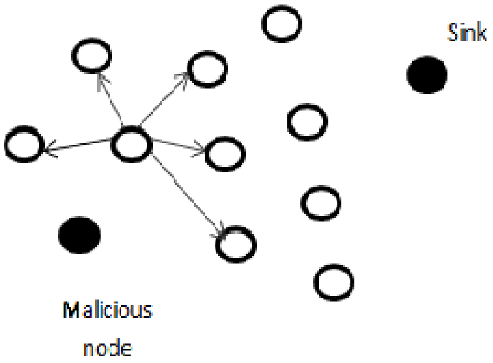

Figure 4: Broadcasting the malicious behaviour

Then other nodes in the network does not send data to the malicious nodes. The neighbours will learn about the malicious behaviour by the broadcast information and hence they can be avoided.

*Infected area:*The area is considered as an infected area if nodes in the network which are one-hop distance to the infected node and which have the possibility to mal-function, those nodes location area is considered as infected area.

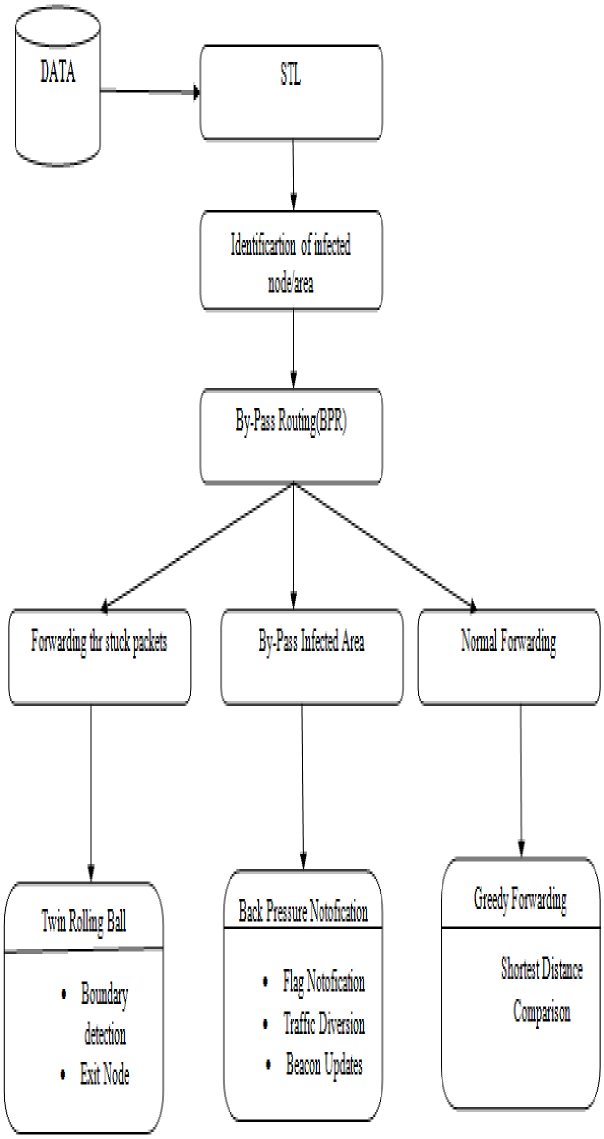

Figure -5 BPR Architecture

The information about the infected node and infected area are used in By-pass routing technique.

3.3 Bypassed Routing:

The main goal of this approach is to get the stuck packets out of the infected region. Second one is to divert the incoming packets from infectedregion. Once the clueabout the infected nodes is obtained from STL technique then that can be used to bypass the infected area and reroute the incoming packets to thee uninfected region. The architecture of the BPR is shown in figure *5*.

By-pass routing in turn has 3 sections

1. Normal forwarding
2. Bypassing the infected area
3. Getting the stuck packets out.

3.3.1 Normal Forwarding:

If there are no infected nodes found then packets are forwarded using greedy forwarding or hop by hop forwarding. The source node knowing the address of the destination or sink node , will wrapup the address of the destination in to packet and forward to its next 1-hop neighbour .The current node that receives the information of destination , it finds its next 1-hop neighbour. This process will continue until it reaches the destination. Incase of the local minima problem BPR method is applied and the process is explained in further sections.

3.3.2 Bypassing the infected areas

This method has to avoidboth thegenerated packets and packets 'on-the-fly' from being directed or routed to infected nodes. Hence, we need to provide an alternative route to detour the affected areas. There are 3 stages in this method.

a) Flag notification of the infected nodes:

The backpressure notification method can be used to notify the source node about the infected node. , the flag is set to 1 if any infected node is detected or set to 0 if no infected node is found. This method sends notification packet via the intermediate nodes that are present within the same route with the infected node to the source node. Hence avoids the unnecessary transmission of the notification packet. The intermediate nodes continue to route the notification packet to its one hopnode until it arrives at the source node. Each node inthis route will delete the corresponding entry of the infected nodes and avoid the sending packets through these nodes again.

b) Traffic diversion :

After the infection flag notification among the nodes, periodic beacon updates occurs between the intermediate nodes. After the beacon update each intermediate node knows its position and distance to their new uninfected 1-hop neighbour. With the use of these uninfected 1-hop neighbours packets can be forwarded to the proper destination. Each intermediate node chooses its 1-hop neighbour based on the closest distance to the destination. This process will continue until it reaches the destination, unless there is no infection notification. This reduces the communication overhead because it requires only knowledge of its 1-hop neighbour and it also saves the time and resources.

c) Beacon updates :

Frequent updates of data in each nodes routing table results in timely delivery of data in the network. In order to minimise the routing overhead we limit the updates for every five intermediate nodes i.e. all the five intermediate nodes updates its routing table one by one after receiving the notification from its neighbour nodes. If source node does not receives the Acknowledgment from the intermediate node. The source node will retransmit after certain threshold time.

3.3.3 Getting the stuck packets out:

Packets in the network may get stuck in some area due to infected nodes and also if there are no nodes available to forward these packets. If this happens then there is more possibility of packet drop. So, to overcome this we propose a solution which includes three stages.

a) Twin Rolling ball:

So when the packets get stuck at the local minima node then the twin rolling ball mechanism is applied[8].

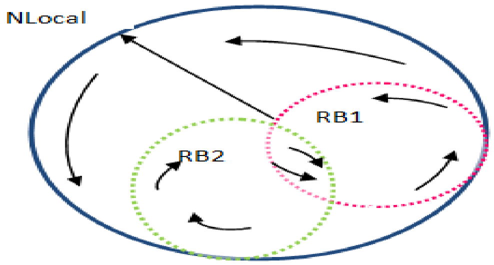

Figure -6 Twin Rolling Balls

Twin rolling ball definition: For all N_i ε N the two similar rolling balls RB$_1 N_i$ (S_i ,$\frac{R}{2}$) and RB$_2 N_i$ (S_i ,$\frac{R}{2}$) is defined as

- The two rolling ball circles attached at N_{local} with its centrepoint atS_i and radius of both circles is equal to$\frac{R}{2}$.

The mechanism of two circles is shown in *figure6*.Using the twin rolling ball mechanism we will select the next hop node to transmit the packet to its destination and flow chart for twin rolling ball is shown in *figure 7*.The two rolling balls attached at theN_{local} node and each of them rotate in clockwise and anti-clockwise direction. First node that is identified by the either of the rolling balls which are in the transmission range of the N_{local} and which is uninfected is selected as next hop. Searching or rotating in two directions ensures the fastest detection of next hop.

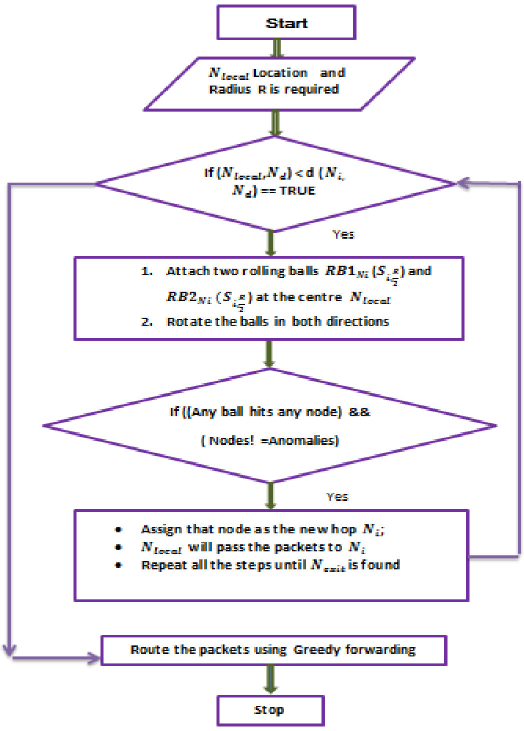
Start
N_{local} Location and Radius R is required
If (N_{local},N_d) < d (N_i, N_d) == TRUE
Yes
1. Attach two rolling balls $RB1_{Ni}$ ($S_{i,\frac{R}{2}}$) and $RB2_{Ni}$ ($S_{i,\frac{R}{2}}$) at the centre N_{local}
2. Rotate the balls in both directions
If ((Any ball hits any node) &&
(Nodes! =Anomalies)
Yes
• Assign that node as the new hop N_i;
• N_{local} will pass the packets to N_i
• Repeat all the steps until N_{exit} is found
Route the packets using Greedy forwarding
Stop

Figure -7 Flowchart of Twin Rolling Ball

The entire procedure of avoiding the infected area from the routing path is given in the algorithm 1

```
Algorithm 1: Avoiding the infected areas
Step 1:Require: Next hop ID, $N_s$ (Source node) address, $N_d$(Destination node) address;
Step 2: Ns initiates the transmission using GF.
Step 3: if (d ($N_j$,$N_d$)< d($N_i$,$N_d$)==TRUE)then
Step 4: Assign$N_j$ as the next hop
Step 5: if (local minima problem is met) then
Step 6: if (packets are stucked! =0) then
        ❖ Twin rolling ball function is applied
Step 7: else
Step 8: Route the incoming or packets on the fly using BPR
Step 9: else
Step 10: Perform the usual GF technique
```

b) Forwarding the stuck packets:

In the proposed technique two identical rolling balls will be attached at local minima node and each of them search for the next hop node in clockwise and anti-clockwise direction. This method compares the distance between first nodes identified by the rolling balls in both the direction. Thenode which has shortest distance and is not infected will be choosen as next hop. The selected node determines the direction of the rest of rotation. The nodes which are all in the range of the local minima node are identified and considered to choose the next hop. The initial node that hits the ball in clockwise is N5, while anti-clockwise is N6 .This method result in the shortest paths and save the energy consumption by unnecessary transmission. The node selection can be understood with the following diagram.

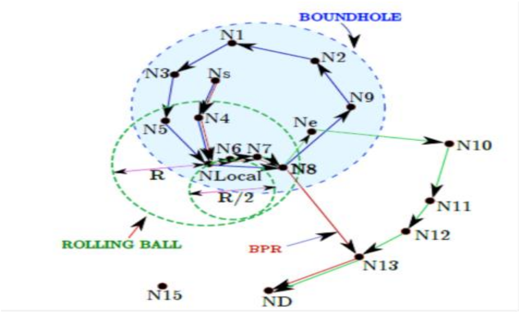

Figure -8 comparison of BPR Routing

c) The exit gate node derivation:

The procedure to find the exit gate node can be found in the algorithm 2. As pictured in the *figure 8* N8 is the last node that intersects the rolling circle. If we choose the previous ones then there could be possibility of routing loops. The transmission range of the $N_{local}$is important in selection of exit node in BPR method. It avoids the longer route. From the exit node we perform the normal greedy forwarding. Since there are no 1-hop neighbours toN_{local}, the next hop is chosen based on GF and i.e. N8. In GAR mechanism the rolling ball is applied at the local minima node and this task continues until the packet reaches the destination node. The total number of visited then it will become 11 in GAR .By using our BPR technique the number hops visited will be 7. Hence avoiding the unnecessary transmissions and proper utilisation of resources.

```
Algorithm 2: The exit gate node
Step 1: Require:Next HopID, Distance to (x,y) location
Step 2: Assuming$N_x$is the current node
Step 3: if (all $N_i$ ε R of Nlocal has been visited) then
Step 4: Assign $N_x$ as exit node
Step 5: if (d ($N_k$,$N_d$)<d($N_x$,$N_d$) == TRUE)
Step 6: then forward the packets to $N_k$
Step7: if(d ($N_j$,$N_d$)<d($N_i$,$N_d$)==TRUE)then
Step 8: Forward the packets to $N_j$
Step 9: Repeat the steps 9 and 10 until destination
Step 10: else
Step 11: Distance of nodes$N_i$and $N_k$ are compared.
Step 12: if(d ($N_i$,$N_d$)<d($N_x$,$N_d$)==TRUE)then
Step 13: Forward the packets to $N_i$
Step 14: else
Step 15: local minima function
```

IV. SAMPLE SCENARIO OFBPR:

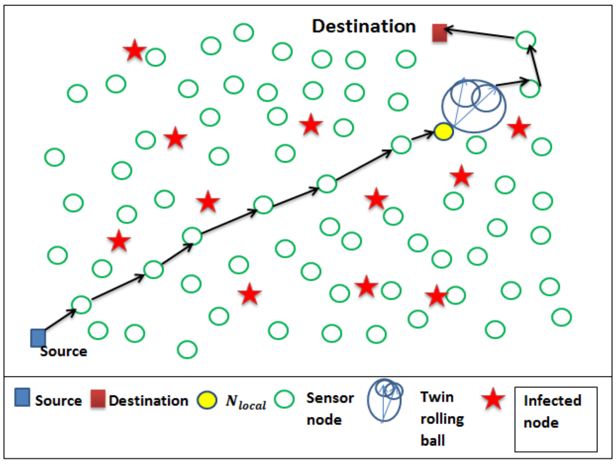

Figure 9: Scenario of BPR

The working process of BPR is as shown in figure 9. The nodes are deployed randomly in the network. The packet is routed from source to destination using GF technique. Once the infected nodes are identified with the help of STL then they are bypassed using BPR. When the local minima situation is encountered then twin rolling ball mechanism is applied and packet is routed to the next hop. Then normal GF is used to route the packet until the packet reaches the destination.

V .CONCLUSION AND FUTURE ENHANCEMENT:

It can be concluded that using By-pass Routing technique and STL,we can avoid the infected nodes.BPR technique improves the performance of the network. It avoids the packets route to the infected nodes and also helps to get the packets out of the stuck nodes which lead to the proper utilisation of the resources.

Future enhancement: After finding the next hop with the help of local minima problem we can apply energy model so that the packets forwarded to the node which has more energy and hence avoiding the packet loss.

VI. REFERENCES:

[1] "Holes in Wireless Sensor Network" by Rajath Bharadwaj and Hitesh sharma , Department of Computer Science and Technology, Lovely Professional University, Punjab, India .

[2] "Wireless Sensor Networks an information processing approach" by Feng Zhao, Leonidas Guibas.

[3] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," SIGMOBILE Mob. Computer Communications. Revised, vol. 9, no. 2, pp. 4–18, Apr. 2005.

[4] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.

[5] "Routing with guaranteed delivery in Ad-hoc wireless networks " by P.Bose, Morin, I.stojmenovic and J.urrutia.

[6] B. Karp and H. Kung, "GPSR Greedy perimeter stateless routing forwireless networks:' in *P m . MobiCm* 2000, FT. 243-254.

[7] G. Qing Fang, Jie Gao and L.J., "Locating and bypassing routingholes in sensor networks," in INFOCOM: 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, 2004, pp. 2458–2468

[8] K.-T. F. Wen-Jiunn Liu, "Greedy routing with anti-void traversal for wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 8, no. 7, pp. 910–922, 2009.

[9] “A simple and effective scheme to find malicious node in wireless sensor network”, by T.Sathyamoorthi, D.Vijayachakaravarthy, R.Divya, M.Nandhini, Master of Engineering, Computer Science and Engineering, Parisutham Institute of Technology and Science, Tamilnadu, India