Providing Efficient Energy to By-Pass Infected Areas in WSN's

Shazia Almas[1], Arudra A[2]

[1]Computer Science and Technology, M.Tech, Rajiv Gandhi Institute of Technology, Bangalore, India

[2]Assistant Professor, Rajiv Gandhi Institute of Technology, Bangalore, India

Abstract: ***Wireless Sensor Network have been the front line innovation in different remote occasion observing applications, particularly in unsafe zones , threatening situations, battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Although several existing methods BOUNDHOLE, GAR, TWIN ROLLING BALL algorithms are used to avoid these problems but their performance are bounded by their limitations. While transmitting the packet the void problem can also occur that makes the packet unreachable towards the destination. This becomes challenge to avoid routing problem in Greedy routing protocol. Especially the active attacks would decrease the Qos parameters of the System , this paper mainly focuses on the After by-passing the packet from the infected area using BPR technique, the Enhancement added further to this is - We are finding the new path from SOURCE to DESTINATION through the best energy-efficient neighbor node. For that, we are setting the energy model using ene.awk and calculating the energy-efficient of best neighbor node. We have to sort the energy file to get the highest energy neighbor node. In final.awkitwill find the new path from source to destination through best energy efficient neighbor node.***

Keywords: Wireless Sensor Network, threatening, smart homes, packet, Greedy routing protocol and energy-efficient.

1. Introduction

A Wireless Sensor Network (WSN) is a gathering of substantial number of independent sensor hubs which are spatially conveyed over a geological territory fundamentally connected to control and screen the physical changes in nature through parameters like pressure, temperature and sound and so on. A WSN system can likewise effectively forward the information between the hubs in bi course with capacity of detecting. Because of a few focal points of these systems it has been utilized as a part of different applications particularly in Military for outskirt observation, mechanical applications and shopper applications etc. Size of the system begins from couple of hubs to hundred and thousand of hubs relying on the application arranged. Every sensor hub has a capacity of detecting the natural changes and convey these data to its neighbor hub inside of its range.

To empower these exercises every hub has bolstered structure, for example, radio handset with an inner receiving wire, a self fueled battery as a vitality source, and a microcontroller to process the information. A WSN can be a homogeneous or heterogeneous system and the size and expense of every hub changes from little to enormous as application differs yet they are restricted by few asset requirements, for example, memory, vitality, rate and correspondence data transmission which makes a system frail while executing progressively.

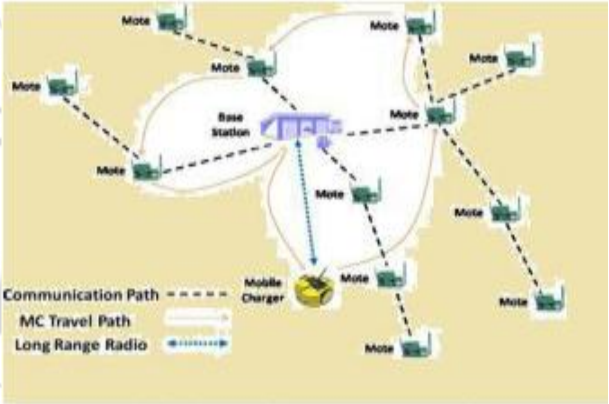


Fig 1 Wireless Sensor Network[WSN]

WSN's more popularly applied in remote monitoring applications, hazardous environment and hostile environment. Any unexpected event may occur in between while transmitting that involves communication of outstanding data to sink node and also they are restricted by energy constraints and other resource limitations. Communication in the WSNs are is crucial because of its state of various intermediate nodes which also forward the data to another node until the destination reaches, this also requires lots of energy consumption by all the node which decrease the life of the node while maintaining connectivity.

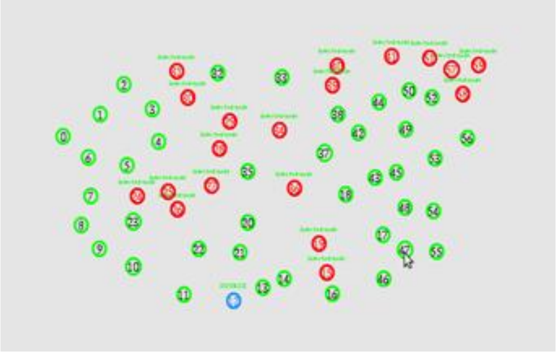


Figure 2: Infected area or node

Data brought by this kind of nodes contain abnormalities that does not mirror exact data .For eg temperature fluctuations observed from normal readings taken. If there are flaws in the node the sensing process will be disorganized, causing serious periodic connection over the whole network, packets may not be forwarded to the destinations by trapping in the infected areas. It introduces the problem of packet loss rate and high consumption of energy in WSNs. Packets carrying important information about occurrence of emergency situation this type of loss of packet could result in severe consequences which affect the whole nation using the network. Anomalous data resulting in incorrect decision making and bad data collected systems in the network need to timely detect corrupted nodes and avoid them which require alternative routes to be reconstructed making incoming packets to detour packets to its destinations by avoiding infected areas.

2. Related Work

WSN research community is considered with a few issues including network lifetime[1] which propose Hybrid Multichip routing HYMN algorithm which is a hybrid of two contemporary multi-hop routing algorithm architectures namely Flat multi-hop routing that utilizes efficient transmission distances and hierarchical multi-hop routing algorithm that capitalizes on data aggregation. In [2] detecting anomalies in sensed data in a WSN is essential to identify malfunctioning nodes in order to minimize communication overhead and energy consumption. In [3] sensor localization by distributed angle estimation propose to estimate the angle of departure (AOD) of the emitted waves at each receiving node via frequency measurement of the local received signal strength indication (RSSI) signal. In [4] Wireless Sensor and Actuator networks(WSANs). Using the mobile sink as an example of the actuator to control the movement of a sink has been adopted by researchers in the past to achieve high efficiency in terms of gathering data from the sensors so proposes a novel method based on set packing algorithm and travelling salesman problem. In [5] MANETs have attracted due to mobility and ease of deployment major challenge is to guarantee secure network, certificate revocation is important, issue of certificate revocation to isolate attackers from further participating in network activity. Most of the routing protocols developed for sensor networks employ greedy forwarding algorithm which forwards a packet to a destination node via one hop neighbor[6].It repeats the process until the packet reaches destination and also efficient in reducing energy consumption.

2.1 Problem Statement

The software corruption, hardware failure and non-favorable operating environment among different nodes in wireless sensor network can reduce the nodes functionality and affect the entire wireless sensor network operations. Node experiencing such a problem is called an infected node. Due to infected node packets cannot be forwarded to destination these packets become lost or stuck in the infected areas. This problem will increase the packet loss rate and energy consumption. The corrupted data in the packets results in false analyses and wrong decision making at end system. Hence a timely detection of the infected nodes and determine the alternative route to divert the traffic from infected area.

3. Proposed Work And Methodology

3.1 By-Passed Routing System

The By-Passed Routing (BPR) technique comprises two parts

- Infected area detection
- By-Passed Routing

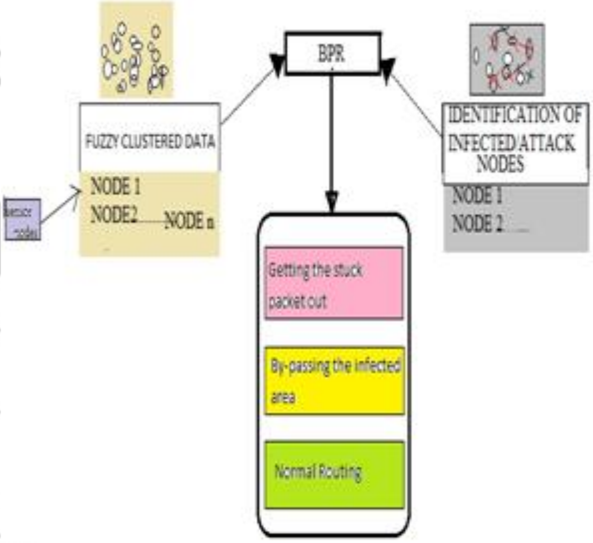
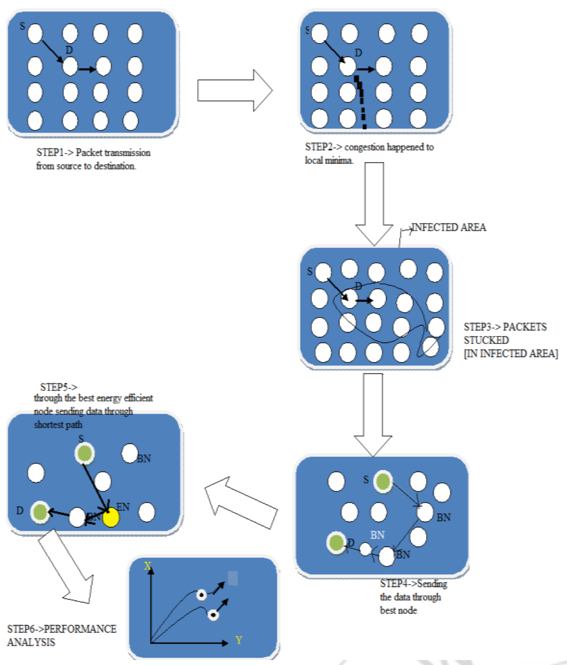

BPR
FUZZY CLUSTERED DATA
NODE 1
NODE2
NODE n
sensor nodes
IDENTIFICATION OF INFECTED ATTACK NODES
NODE 1
NODE 2
Getting the stuck packet out
By-passing the infected area
Normal Routing

Figure: System Architecture of BPR

First part identifies the infected nodes by Fuzzy Data Clustering to detect anomalies. This method is chosen as it evaluates anomalous data over various sensor nodes. A centric data point view with fuzzy cluster is correct when evaluating a node is infected or not whether through malware attack, hardware malfunction or software corruption. Infected node information is then used for traffic diversion in the proposed BPR technique. The innovation of BPR approach relies on introduction of twin rolling ball technique that recognize the next one hop neighbors immediately than the GAR approach. Getting the trapped packets out of infected region is other contributes of BPR.

Procedure of BPR:


S
D
STEP1-> Packet transmission from source to destination.
S
D
STEP2-> congestion happened to local minima.
INFECTED AREA
S
D
STEP3-> PACKETS STUCKED [IN INFECTED AREA]
S
BN
BN
D
BN
STEP4->Sending the data through best node
STEP5-> through the best energy efficient node sending data through shortest path
S
BN
D
EN
BN
X
Y
STEP6->PERFORMANCE ANALYSIS

3.2. Fuzzy Data Clustering

Infected node: The node Ni from the given set of sensor nodes N= [N1,N2,……Nn] is considered as infected if it does satisfies the following condition

- Contains some outlying fluctuation points which can be classified as anomalous with its fraction over normal measurements is >=10% of its aggregated readings over a considered time window δT.
- **Infected area:** Given a subset (n) of WSN sensor nodes (n ϵ N), which are over a particular spatial area A, that area is considered as an infected area if and only if;
- All the sensor nodes in n satisfy the criteria for Definition of infected node.
- Each node is within one hop communication distance of at least one other node in n.

Fuzzy data clustering method is used for detecting the anomaly in the sensed data. Based on membership values fuzzy data clustering method make the partition of data into clusters and in this method each data element can part of more than one cluster. The membership value represent degree which data element belonging to the particular cluster.

The FCM algorithm try to divide a list of n elements X={X1,X2,….,Xn} into a C fuzzy clusters based on certain condition. The output of algorithm is a set of C cluster centers C={C1,C2,….,Cn} and membership matrix W=wab where wab belongs to [0,1] a=1,….n, b=1…….C, where wij indicate the strength of association between element Xa and the cluster Cb. The FCM (fuzzy c – means clustering) goal to minimize an objective function (jm) .

$$J_m = \sum_{a=1}^{n} \sum_{b=1}^{C} w_{ab}^{m} \|X_a - C_b\|^2$$

$$\text{Where } w_{ab} = 1 \div \sum_{K=1}^{C} (\|X_a - C_b\| \div \|X_a - C_k\|)^{2 \div (m-1)}$$

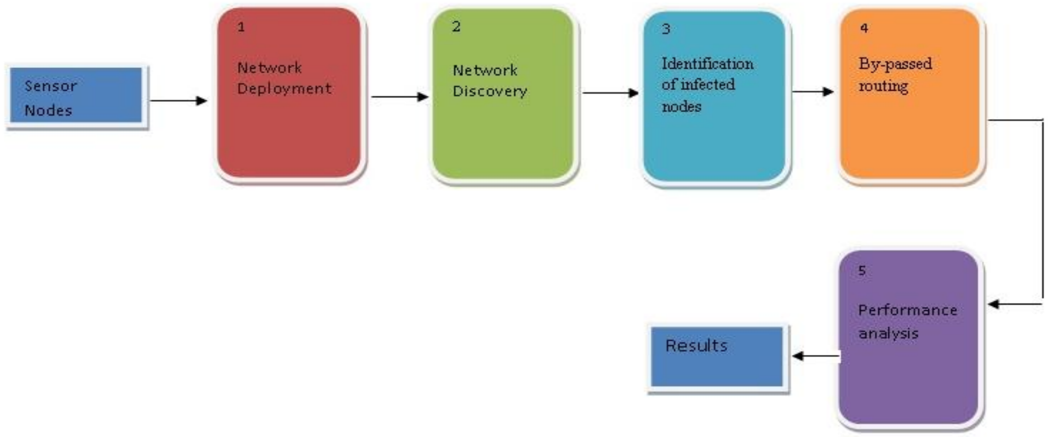
The fuzzifier m identifies the degree of cluster fuzziness. A smaller m results in larger membership's w_{ab} values assigned to data means whose intensities are close to the particular centroid and larger m value results in smaller membership's web values assigned to data means data is far from the centroid. The membership's w_{ab} converge to 0 or 1. The value of m is normally set to 2 when there is a no experimental knowledge.

The membership degree of any data point X in kth cluster is represented by wk(X). In FCM, the mean of membership degree of every data points in the cluster is centroid of that cluster.

$$C_k = \sum_x w_k(X)^m X \div \sum_x w_k(X)^m$$

4. Data flow diagram of BPR

The proposed By-Passed Routing (BPR) technique consists two main parts, namely infected area identification and bypassed routing.



Fuzzy-C-Mean algorithm 1

Step1. Select a number of clusters.

Step2. Randomly assign membership value for each data point and centroid for each cluster.

Step3. Iterate until the algorithm meet its condition (that is, the variation of values between two iterations is no more than €, the given sensitivity threshold):

Step4. Determine the center of every cluster. Step5. For every data element, determine its degree of membership within a cluster [4-5].

2.2. By-Passed Routing (BPR)

The aim of this technique is first to get stuck packets out of the infected regions. Second we divert the incoming packets from infected region. Once the information about the infected region is obtained from fuzzy data clustering than that can be used to by-pass the area and reroute the incoming packets to uninfected region. This section consists of three different parts: Getting the Stuck Packets Out, By-passing the infected areas, and Normal Routing.

Algorithm 2: Avoiding Infected Areas

```
Step 1: Require: NextHopID, Ns, ND Address;
Step 2: Ns initiates transmission using GF Algorithm;
Step3: if (d(Nj, ND) < d(Ni ,ND) == TRUE) then
Step 4: Assign Nj as the next hop;
Step 5: if (Local Minima problem is met) then
Step 6: if (Stuck Messages != 0) then
    • Call the Twin Rolling Balls function;
    • Get the Stuck Messages out;
Step 7: else
Step 8: Route the incoming packets using BPR;
Step 9: else
Step 10: Perform the GF algorithm;
```

Getting the Stuck Packets Out: Some packets are stuck in the region due to the infected nodes and also there is no node available for forward these packets to next hop. If no alternative path arrangement made for these packets than there is high risk of being dropped. This section composed of three parts: Twin Rolling Balls, Forwarding the Stuck Packets, and the Derivation of Exit Gate Node.

The Twin Rolling Balls: For all Ni϶ N the two similar rolling balls RB1Ni(Si, R/2) and RB2Ni(Si, R/2) is defined by The two rolling circles attached at the NLocal with its

- Center point at Si and radius of both circles is equal to R/2. {RBiÑi(Si, R/2)⌒N}= NULL indicate the node Nk ϵ N should not be present in the open space within the two rolling balls ({RBiÑi(Si, R/2)⌒N}).

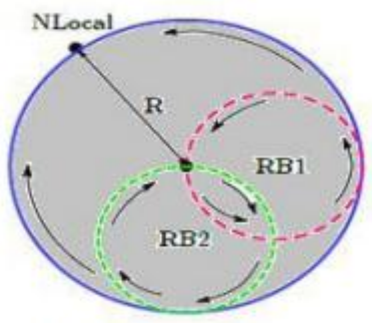


Fig 5 Two Rolling ball operation

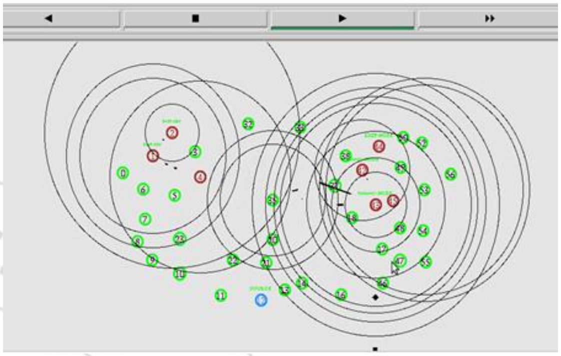


Figure 5.1: Twin rolling ball technique is used finding the best- neighboring node where the packets are getting by-passed using by-pass routing

After infected node and twin rolling ball is done, the back trace message must be send to source node to inform its infected and stop sending the packet to the node, to bypass the node and take alternative route. This alternate path again depends upon the parameter taken for the other nodes to satisfy the condition and taken in the loop with normal forwarding algorithm.

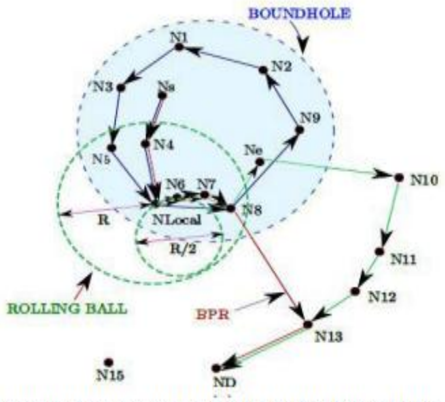
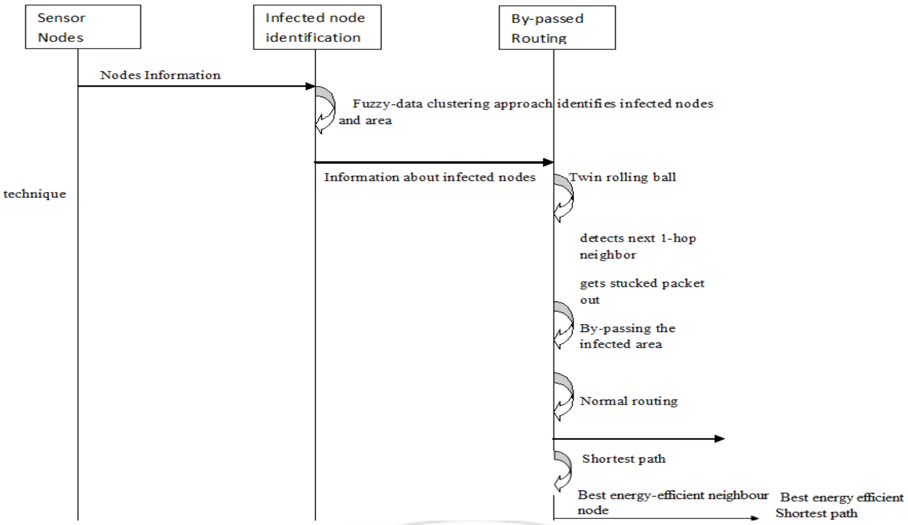


Fig 6 Example of constructing path using Rolling ball technique

In fig the ball will attach at Ne , it will roll and hit N10.This process continues till the packet reaches destination node (ND).This method unnecessary visits to other nodes(Ne ,N10,N11,N12) While there is another shortest route to destination. In contrast the BPR method will choose N8 as an exit gate node. The selection of this exit gate node is based on transmission range covered by Nlocal. Ne node excludes as exit gate node avoiding taking longer routes. From node 8 it will proceed with normal forwarding using GF algorithm.

Sequence diagram of BPR:


Sensor Nodes
Infected node identification
By-passed Routing
Nodes Information
Fuzzy-data clustering approach identifies infected nodes and area
Information about infected nodes
technique
Twin rolling ball
detects next 1-hop neighbor
gets stucked packet out
By-passing the infected area
Normal routing
Shortest path
Best energy-efficient neighbour node
Best energy efficient Shortest path

5. Results and Discussion

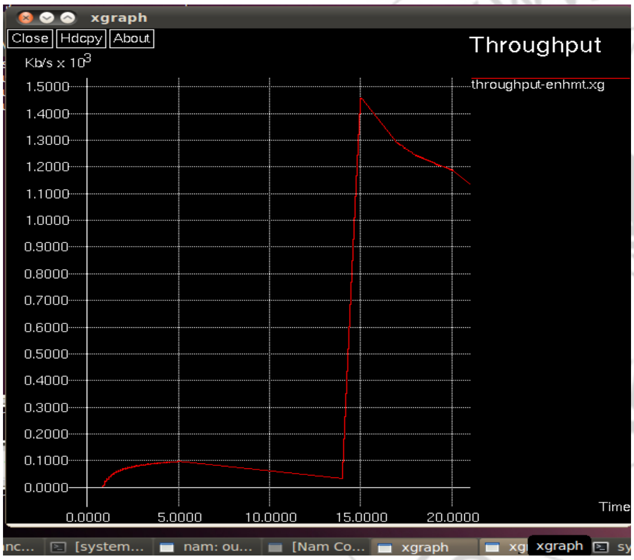


Figure: Throughput graph of enhancement.

Dark blue node shows the best energy efficient node among all the best nodes and it also finds the new path from source to destination through best efficient neighbor node.

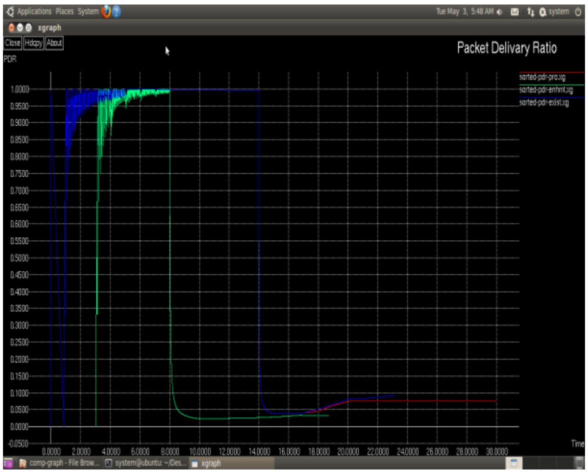


Figure: PDR comparisons

6. Conclusion and Future Work

In this work, the efficiency of the By-Passed Routing technique where it avoids the infected nodes in network is seen thereby improving the overall performance of network. The infected area comprising of infected nodes called also as anomalous nodes are detected by fuzzy data clustering technique in which first clustering is performed and infected node is calculated based on threshold value in energy model. This information is used by the BPR technique where it finds the alternate path to transfer of packets from source node to destination node with the help of twin rolling balls which define the next forwarding node and reduces the false boundary detection seen in existing rolling ball technique.

After by-passing the packet from the infected area using BPR technique, the Enhancement added further to this is - We are finding the new path from **source** to **destination** through the best energy-efficient neighbor node. For that, we are setting the energy model using ene.awk and calculating the energy-efficient of best neighbor node. We have to sort the energy file to get the highest energy neighbor node. In final. awkitwill find the new path from source to destination through best energy efficient neighbor node.

References

[1] 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.

[2] A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato, "HYMN: A novel hybrid multi-hop routing algorithm to improve the longevity of wsns," IEEE Transactions on Wireless Communications, Vol. 11, no. 7, pp. 2531–2541, July 2012.

[3] N. Arad and Y. Shavitt, "Minimizing recovery state in geographic ad hoc routing," IEEE Transactions on Mobile Computing, Vol. 8, No. 2, pp. 203–217, 2009.

[4] D. Chen and P. K. Varshney, "On-demand geographic forwarding for data delivery in wireless sensor

networks," Computer Communications, Vol. 30, No. 1415, pp. 2954 – 2967, 2007.

[5] M. Ahmadi Livani and M. Abadi, "An energy-efficient anomaly detection approach for wireless sensor networks," Proceedings of 5th International Symposium on Telecommunications, pp. 243–248,2010.

[6] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," Association for Computing Machinery Special Interest Group on Mobility of systems, Users, Data, and Computing (ACM SIGMOBILE), Review 9, No. 2, pp. 4–18, April. 2005.

[7] Q. Fang, J. Gao, and L. Guibas, "Locating and bypassing holes in sensor networks," Mobile Networks and Applications, Vol. 11, No. 2, pp. 187–200, 2006.

[8] S. Lai and B. Ravindran, "Least-latency routing over timedependent wireless sensor networks," IEEE Transactions on Computers, Vol. 62, No. 5, pp. 969–983, 2013.

[9] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato, "Cluster-based certificate revocation with vindication capability for mobile ad hoc networks," IEEE Transaction on Parallel Distributed System, Vol. 24, No. 2, pp. 239–249, Feb. 2013.

[10] S. Chen, G. Fan, and J. hong Cui, "Avoid 'void' in geographic routing for data aggregation in sensor networks," International Journal of Ad Hoc and 2016.

[11] Ashwini and A. S., "Information dissemination between nodes of different intersections intersection in city environment using hop greedy routing protocol (BAHG)," Int. J. Ethics Eng. Manag. Educ., vol. 1, no. 4, pp. 232–236, Apr. 2014

[12] S. Subramanian, S. Shakkottai, and P. Gupta, "On optimal geographic routing in wireless networks with holes and non-uniform traffic," in Proc. IEEE 26th Int. Conf. Comput. Commun., May 2007, pp. 1019–1027

[13] H. Nakayama, N. Ansari, A. Jamalipour, and N. Kato, "Faultresilient sensing in wireless sensor networks," Comput. Commun., vol. 30, no. 11-12, pp. 2375–2384, Sep. 2007.