Hole Detection Routing Protocol for Wireless Sensor Networks

Anju Arya[1], Nisha Nehra[2]
[1]Computer Science and Engineering, Deenbandhu Chhotu Ram University of Science and Technology, Murthal
[2]Computer Science and Application, DAV College for Girls, Yamunanagar
Haryana, India

Abstract : In wireless sensor networks, optimal data routing is of prime importance task while tackling the limited resources constraint at the same time. Apart from limited resources constraint, there are others problems too which affects network's lifetime adversely. One such major problem is holes problem in the network. The presence of hole leads to non-optimal usage of limited resources. In our work, we have proposed hole detection algorithms to detect holes or dead zones in the network. The simulation results have shown the ability of our algorithms to detect hole(s) when it occurs. Our work on holes focuses on coverage hole detection and routing hole detection.

Index Terms - Reinforcement Learning (RL), Wireless Sensor Network (WSN), Routing Protocols, Q learning, Holes.

I. INTRODUCTION

A wireless sensor network (WSN) [1] is a network of autonomous sensors deployed in a structured or unstructured fashion to monitor the physical environment and then cooperatively transfer the gathered information through the network to the sink via intermediate sensor nodes. The sensors nodes are usually deployed densely to gather as much relevant information as possible for the accurateness and correctness of the collected data. The technological advancements such as Micro-Electro Mechanical Systems (MEMS) have increased the interest in wireless sensor networks tremendously. Apart from the physical environment which could create problems in sensor functioning, the sensor networks have to face yet another major challenge of limited resources. Since deployed sensor nodes can't be accessed all the time for checking out their hardware functioning or recharging batteries, thus it is very important to use the limited energy available efficiently for making the sensor node perform its function properly. The presence of holes may lead to wastage of resources and decrease in service quality like increased end-to-end delay. Thus, resource management is of uttermost importance in wireless sensor networks.

In this paper, we present hole detection algorithms to detect holes in the sensor network. Hole problem is one of the major research challenge. It affects the network performance by hindering the monitoring or tracking activities of the target area or object. This results in inaccurate and inefficient data gathering and analysis. Holes can be grouped into 4 categories based on the type and cause of its formation, namely as coverage holes, routing holes, jamming holes, and sink/black/worm holes. Some of the hole detecting methods are mentioned in TABLEI.

II. OVERVIEW

The main objectives of the protocol is hole detection. The routing protocol uses an optimal routing is a routing behavior in which the selected route is the best available or optimized route in terms of total energy cost and transmission delay among the available ones for a particular source to destination(s) pair. But, even after using the optimal routing criteria while ensuring uniform energy distribution, holes problem may occur due to sudden high data load conditions or transmissions or during the degrading phase of the network. A hole is created in the network when a group of nodes stops sensing data and communicating with the other nodes in the neighborhood. Then, a hole detection algorithm can be used to provides detailed statistics about the kind and cause of hole formation.

TABLE I. A summary of various hole types

Hole Type	Reason	Depends on	Hole Detection /Discovery
Coverage holes	• Insufficient sensor deployment to cover target area	• Application requirement • Target environment	• Voronoi diagrams [2, 3, 4] • HSTT [5]
Routing holes	• Voids due to non uniform deployment • Sensor failure due to no battery, faulty sensor, or physical destruction.	• Deployment strategies • Battery level • Target environment	• BOUNDHOLE [6]
Jamming holes	• Jammers • Faulty nodes occupying communication channel continuously and preventing other nodes to communicate. • Target or tracked object characteristics such as noise, jammer-equipped, etc.	• Presence of jammers • Defective or malicious sensors. • Targets object characteristics.	• JAM [7]
Sink/Black/ Worm holes	• Denial of Service attacks • Insecure wireless channel • High resource contention for limited channel bandwidth and communication channel access	• Presence of malicious sensors	• Sink hole: Packet leashes [8], SECTOR [9], Nagai, et al. [10] • Black hole: Sun, Bo, et al. [11]

The hole formed consists of nodes in one of the following conditions or states:

A. Dead nodes

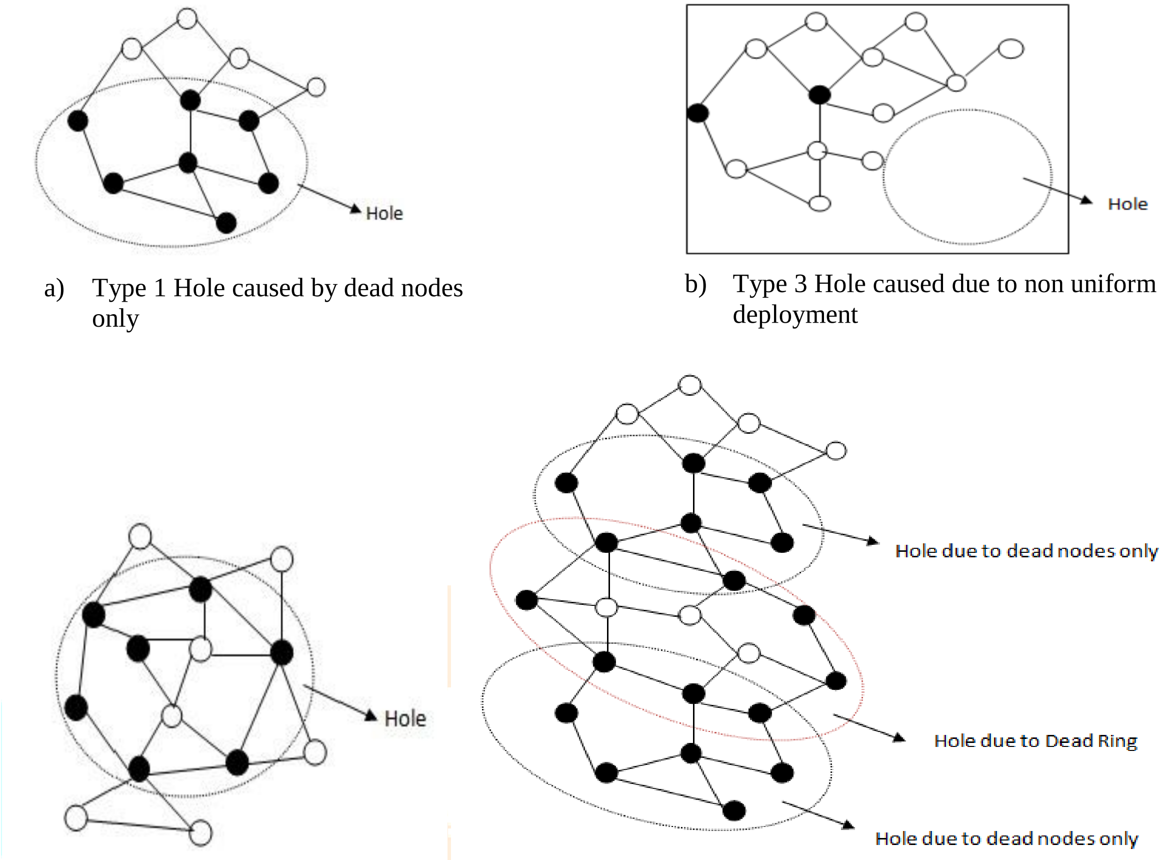
The hole formed consists of dead nodes only, see Fig 1(a). Such type of hole is formed when one or few of the neighboring nodes of a node dies and the data load on those nodes gets transferred to that node or on other good state neighbors.

B. Dead and inaccessible nodes

The hole formed consists of dead nodes only, see figure 2. This hole is formed when a ring of dead holes surround some “good” or “working” state nodes making them inaccessible. Such type of hole is formed when two or more optimal paths are chosen frequently during routing and under high loads, the nodes on that path along with some of their neighbors looses their energy and die. A dead ring is formed if any of such two or more routes consisting of dead nodes shares two or more common dead nodes, see first figure of Fig 1(c). However, such a case occurs rarely because of the optimal selection of next hops in our approach, which prevents the selection of best available routes again and again. The second case, which might result in the formation of a dead ring, is when few or more working nodes lying between the two holes dies resulting in the formation of a dead ring, see second figure of Fig 1(c). This might happen during the selection of working nodes around the holes boundary. This situation can hamper the whole network if the network or cluster is small or not large enough to tolerate two or more holes and may not be able to continue with its normal functioning or routing activity. The second case must be handled immediately, especially for small or medium sized networks or clusters.

C. No sensor node due to poor deployment

This case arises when deployment is not uniform in an area or the environment is harsh or hostile such as deep wild forests, battlefields and volcanic mountains. Such type of hole contains no sensor nodes at all, see Fig 1(b).



a) Type 1 Hole caused by dead nodes only

b) Type 3 Hole caused due to non uniform deployment

c) Type 2 Hole caused by dead ring

Fig. 1 Various types of Holes formed

The hole detected must be handled timely before the whole network get affected to ensure proper service delivery throughout the network's lifetime. The delay in handling hole can be seen in the form of increased data delivery for some period of time, which might be short or long depending on time taken for action or decision to mitigate holes problem. If optimal routing is the first step towards maximizing or increasing network's lifetime, then hole mitigation is the second step in response to the failure of the first step to increase network's lifetime or avoid network degradation due to lack of power and resources.

III. HOLE DETECTION

Hole detection is done at base station site periodically. During the routing process, if any sensor node is about to die, then just before death it broadcasts a DEATH message to all its neighbors. The neighboring nodes receiving the DEATH message removes all the entries of the dead node from their routing table. The neighboring nodes also sends the information regarding dead neighbor's coordinates to the base station in the form of "Hole info" data.

The base station runs hole detection algorithm periodically on the gathered networks data. It uses dead nodes information collected in time for hole detection. If a hole is detected, then the base station can send information about the dead nodes on the hole boundary along with the type of hole detected to the main controller, if such an arrangement is done.

< deadnode_coord_list, type>

The coordinates of the dead nodes on the boundary can be plotted on a graph to view the shape of the hole area.

The information regarding the hole area such as center of the ellipsoidal area enclosing the hole area and the diameters along the x-axis and y-axis of the ellipse, figure4, can also be provided easily.

Center : (hx, hy)
Diameter along x-axis : d1
Diameter along y-axis : d2
Reference coordinates : (bx, by), for cluster or network in case of virtual coordinate system

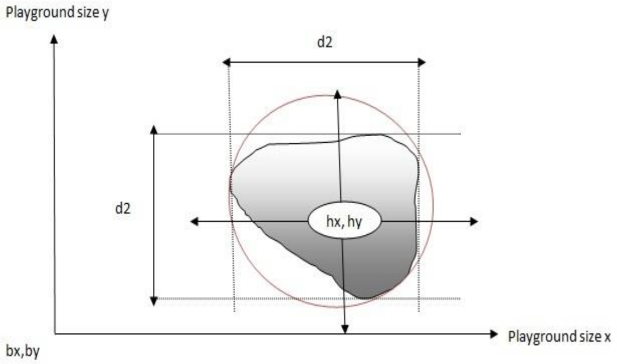


Fig. 2 A plotted hole area on a graph

The above information is useful for deployment of both uniform type (in case of holes consisting of dead nodes or no nodes) and non-uniform type (along the perimeter for dead rings). When the base station runs hole detection algorithm on the network information collected, it will produce the information shown in Fig 2 as output in a file.

In general, a hole boundary refers to the working nodes creating a boundary along the sides of dead nodes cluster and they can be used to divert network traffic or change the route of packets, which were supposed to pass through dead nodes according to their regular route. There can be two kinds of boundary nodes. One is network boundary nodes, which reside on the boundary of the network and the other is hole boundary nodes, which resides on the boundary of the hole(s) and enclose the destroyed sensors only. In this work, We are concerned with hole boundary only. In our algorithm, hole boundary nodes refers to the dead nodes making the boundary of the dead nodes cluster

IV. HOLE DETECTION ALGORITHM

The presence of holes in the network is detected by running two different algorithms. One algorithm detects routing holes present in the network and the other algorithm detects coverage hole in the network.

A. Routing Hole Detection

The algorithm detects holes in two steps. The first step detects hole formed by a group of dead nodes only. If a dead node with all its neighbors dead too and may be the neighbors of its neighbor are also dead and so on is detected, then we declare this group of dead nodes as a hole. In the second step, those holes are detected, which are formed due to dead rings surrounding some good inaccessible nodes.

B. Coverage Hole Detection

The coverage hole is detected by taking each sensor node location one by one.
Taking each location as reference, the presence of nodes is detected in all the four directions or quadrants. The size of the quadrant is initially set equal to the transmissions range. If no node is detected in a quadrant area, then its size or range is increased incrementally with some value and again the presence of nodes is checked for this new rectangular area. This process is continued for each quadrant, with reference to a node's location, until either one or more nodes are detected in the extended area or the network boundary is reached.

V. Simulation Results

A. Hole detection results

The sample network used for analysis is a connected 100-node topology on a field size of 150x150m, with a maximum transmission or communication range of 10m. The data requests are sent after every 10sec by all the sinks and the sources send data after every 2sec.

A hole detected can be categorized into following types based on the state of sensor nodes forming it.

Type 1. *Dead nodes only*
Type 2. *Dead and inaccessible nodes (due to dead rings)*
Type 3. *No sensor node deployment*

Result 1. For Hole Type 1

Consider the sample network shown in Fig 3(a). Now, suppose some of the nodes are dead. In this case, a hole is detected. The area of the hole detected is shown in graph by plotting the coordinates of the dead nodes of the hole on the graph as shown in figure 3(b). Figure 3(c) shows the hole area more clearly by blackening the sub-area covered by the dead nodes of that hole.

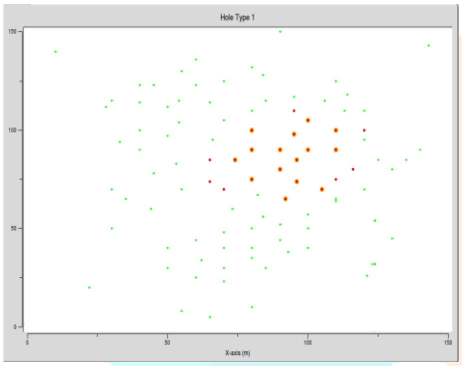


Fig 3(a) A Graph displaying some dead nodes (red/yellow) in sample network of figure 20 and without connections

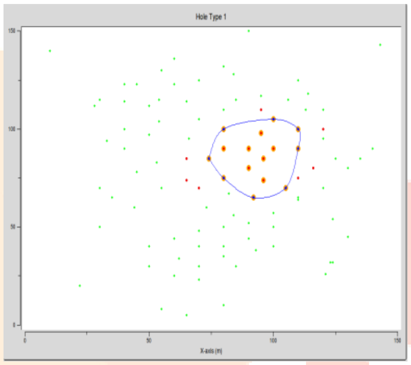


Fig 3(b) A Graph displaying the dead nodes (yellow) of the hole detected

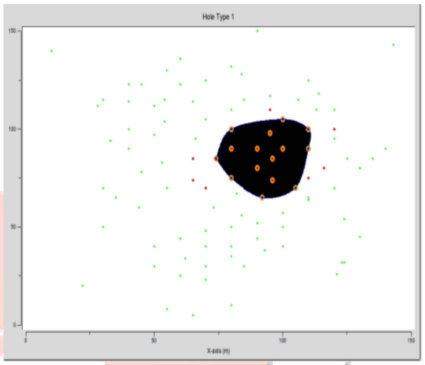


Fig 3(c) A Graph displaying the hole area shown in Fig 3(b). as blackened portion

Results of Hole Type 1

Result 2. For Hole Type 2

Consider the sample network shown in Fig 3(d). Now, suppose some of the nodes are dead. In this case, two dead rings are detected forming a hole. Then the area of the holes detected is shown in graph by plotting the coordinates of the dead nodes of the holes on the graph with connected lines as shown in Fig 3(e). The sub-areas enclosed by the two rings shown in Fig 3(e) are hole areas and it is shown more clearly in Fig 3(f) as blackened area.

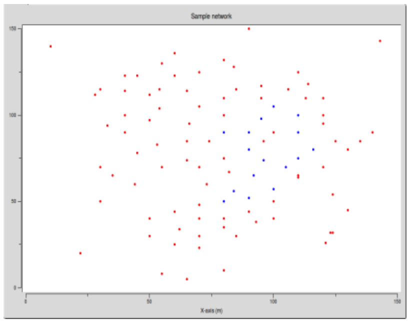


Fig 3(d) A Graph displaying some dead nodes (blue) in sample network of figure 20 and without connections

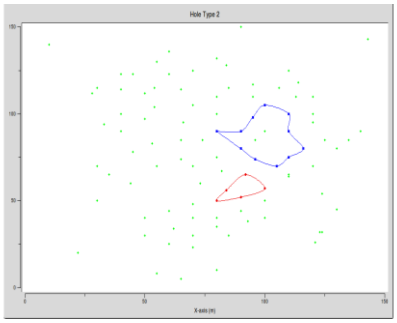


Fig 3(e) A Graph displaying the holes detected, 2 dead rings (blue & red) in this case

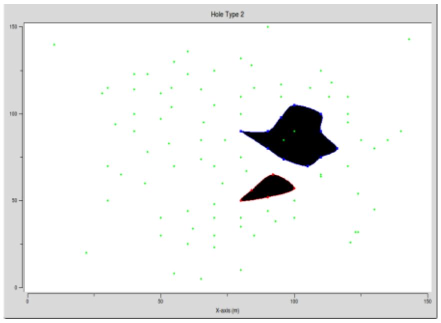


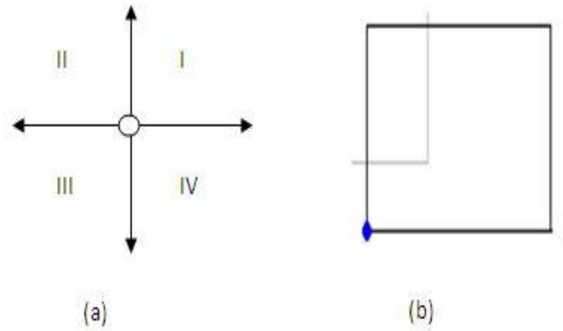
Fig 3(f) A Graph displaying the hole area of the 2 holes in Figure 3(e). as blackened portion

Results for Hole Type 2

Result 3. **For Hole Type 3**

This type of hole is detected after the deployment of sensor nodes when all the nodes are in working state i.e. at the initial stage of the network when there are no dead nodes. There is no need to check for this hole periodically as for the above two type of holes. The non-uniform deployment is detected by examining every sensor node quadratically i.e. quadrant wise taking sensor node's location as the center point or reference as shown in Fig 3(g,a). The range of communication void for a particular node is shown through a rectangle, whose length and breadth gives the range of the void area or hole area, see Fig 3(g,b).

For the sample network shown in Fig 3(h), the communication voids as a result of non-uniform deployment are shown in figure 30 for every affected sensor node.



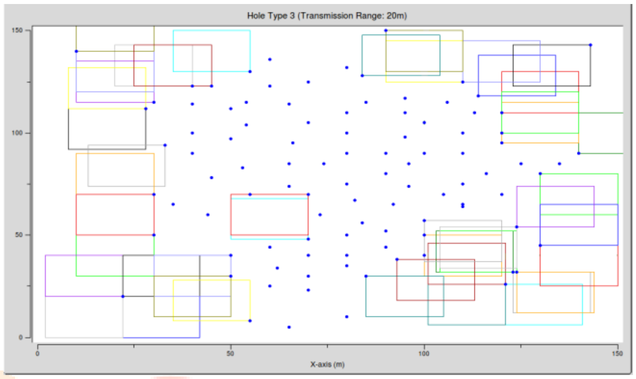


Fig 3(g,a) Displays the quadrant system taking a node's location as reference and Figure 3(g,b) Represents a communication void using a rectangle shape for the blue colored node.

Fig 3(h) A Graph displaying the communication voids or holes w.r.t. sensor nodes locations

Results for Hole Type 3

Fig. 3 Results for Hole Type1, 2, and 3

VI. CONCLUSION

The reinforcement learning approach used by our protocol has proved to be effective in selecting optimal paths during routing. The simulation results have clearly demonstrated the ability of our protocol to support sink mobility, handle node's failure, and detect holes occurring in the network.

REFRENCES

[1] Malik Tubaishat and Sanjay Madria, "Sensor Networks: an overview," in IEEE 2003.

[2] Guiling Wang, Guohong Cao, and Tom La Porta. Movement-assisted sensor deployment. In IEEE INFOCOM 2004, June 2004

[3] G. Wang, G. Cao, P. Berman, T.F.L. Porta, "Bidding protocols for deploying mobile sensors", IEEE Transactions on Mobile Computing 6 (5) (2007) 515–528.

[4] Aurenhammer, Franz, and Rolf Klein. "Voronoi diagrams." Handbook of computational geometry 5 (2000): 201-290.

[5] Babaie, Shahram, and Seyed Sajad Pirahesh. "Hole detection for increasing coverage in wireless sensor network using triangular structure." arXiv preprint arXiv:1203.3772 (2012).

[6] Fang, Qing, Jie Gao, and Leonidas J. Guibas. "Locating and bypassing routing holes in sensor networks." INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. Vol. 4. IEEE, 2004.

[7] Anthony D. Wood, John A. Stankovic, and Sang H. Son. JAM: A jammed-area mapping service for sensor networks. In 24th IEEE Real Time System Symposium (RTSS'03), pages 286.298, Dec 2003.

[8] Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks, in: Proc. Of Infocom2003. San Francisco, CA, USA, April 2003.

[9] S. Capkun, L. Buttyan, J. Hubaux, SECTOR: Secure Traking of Node Encounters in Muti-hop Wireless Networks, in: proc. Of SASN 2003.Fairfax, Virginia, October 2003.

[10] E. C. H Ngai, J. Liu and M R. Lyu, "On the intruder Detection for Sinkhole Attack in Wireless Sensor Networks," Proc. IEEE ICC, 2006.

[11] Sun, Bo, et al. "Detecting black-hole attack in mobile ad hoc networks." Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492). IET, 2003.