HOLE DETECTION AND HEALING FOR A RoI IN WIRELESS SENSOR NETWORKS

Divya K Suku , Phini Ann Philip

PG Scholar, Department of ECE, CAARMEL Engineering College, Pathanamthitta, Kerala
Assistant Professor, Department of ECE, CAARMEL Engineering College, Pathanamthitta, Kerala

E-mail:divyasuku91@gmail.com

Abstract: Sensor technology is one of the fast growing technologies in the current scenario. And it has wide range of application also. The ability of sensors to work without being monitored by any individual is its unique quality. Wireless sensor network comprise of small sensors which have minimum communicational and computational power. Several anomalies are present in WSNs. One such problem is a hole. Area devoid of any node can be referred to as a hole. This degrades the performance of the whole network. It affects the routing capability of the network very badly. The formation of holes in a WSN is unavoidable due to the inner nature of the network. This paper deals with detecting and healing such holes in an on demand basis.

Keywords: Wireless sensor network, holes, hole detection, coverage, hole healing

INTRODUCTION

A wireless sensor network is composed of tiny sensor nodes. Each sensor node is capable of sensing some phenomenon, doing some limited data processing and communicating with each other. These tiny sensor nodes are deployed in the target field in large numbers and they collaborate to form an adhoc network capable of reporting the phenomenon to a data collection point called sink or base station. These networked sensors have many potential in civil as well as military applications that is, they are used for environmental monitoring, industrial monitoring and they are also utilized for object tracking. Sensor nodes are even used for health related applications etc.

Several anomalies can occur in wireless sensor networks that impair their desired functions such as communication and sensing. One such anomaly is a hole. Destruction of nodes causes holes. Area devoid of any node is termed as a hole. Different types of holes are present namely coverage holes, routing holes, jamming holes, black holes/sink holes etc. WSN are deployed in hostile environment and left unaltered for a relatively longer period of time. At times a group of sensors fail to carry out the network operations. Such nodes are termed as destroyed node. In sensor network we come across a type of node termed as faulty node. A faulty node is a node which gives result which significantly deviate from the results of its neighboring nodes. The emergence of holes in the network is unavoidable due to the inner nature of WSNs, random deployment, environmental factors, and external attacks. Thus, an event occurring within these holes is neither detected nor reported and, therefore, the main task of the network will not be completed. Thus, it is primordial to provide a self-organizing mechanism to detect and recover holes. This paper seeks the problem of hole detection and healing in an on demand basis.
Some of the major reason for node destruction and hole creation are:

- Power depletion: Each sensor node is equipped with power battery. Once depleted it is not an easy task to recharge the nodes.
- Physical destruction: Physical destruction of nodes due to some environmental reason cause a hole in the network.
- Existence of obstacles: An example for such a situation is a sensor node fell in a pond where its task is to monitor forest fire. This make the inactive for the purpose and a hole is created.
- Lower density regions: Nodes that fall in the lower density region acts as isolated nodes and form holes.

PROBLEM DEFINITION

There has been much researches on hole detection problem as it is one of the major problem of wireless sensor networks. In almost all process the first method id to detect the topology of the network. And it is done by many means. And also the type of the hole has to be identified. We formally define here various types of holes and their characteristics.

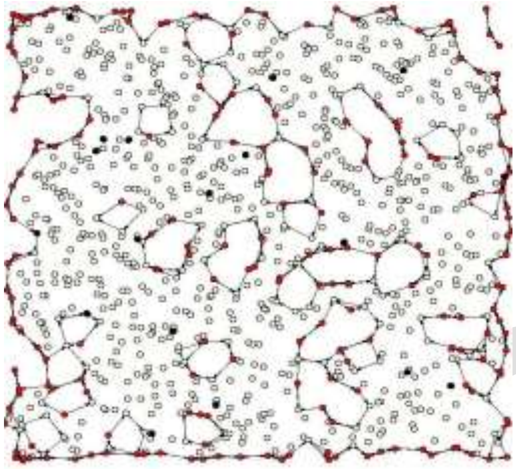
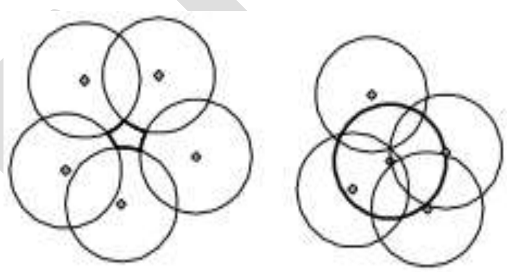


Fig.1 Holes in a WSN

1 Coverage Holes

Given a set of sensors and a target area, no coverage hole exists in the target area, if every point in that target area is covered by at least k sensors, where k is the required degree of coverage for a particular application (see Fig. 2). It is pertinent to mention that the coverage hole problem defined is dependent on application requirements. Some applications may require a higher degree of coverage of a given target area for fault tolerance/redundancy or for accurate target localization using triangulation-based positioning protocols [7] or trilateration based localization [8].

The sensing coverage of a sensor node is usually assumed uniform in all directions and is represented by unit disc model (Fig. 1). However, this idealized model is based on unrealistic assumption: perfect and same coverage in a circular disc for all the sensors. Moreover, the coverage not only depends on the sensing capability of the sensor but also on the event characteristics [9] e.g. target detection of military tanks as compared to detection of movement of soldiers depends on the nature and characteristics of event as well as the sensitivity of the sensors involve\ed.



(i) (ii)

Fig.2(i). Coverage hole with unit disk sensing model (ii). Sensor with dark gray sensing circle is necessary if degree of coverage required is 2

2 Routing Holes

A routing hole consist of a region in the sensor network where either nodes are not available or the available nodes cannot participate in the actual routing of the data due to various possible reasons. These holes can be formed either due to voids in sensor deployment or because of failure of sensor nodes due to various reasons such as malfunctioning, battery depletion or an external event such as fire or structure collapse physically destroying the nodes. Routing holes can also exist due to local minimum phenomenon often faced in geographic greedy forwarding. Forwarding here is based on destination location. In Fig.3, a node *x* tries to forward the traffic to one of its 1-hop neighbor that is geographically closer to the destination than the node itself. This forwarding process stops when *x* cannot find any 1-hop neighbor closer to the destination than itself and the only route to destination requires that packet moves temporarily farther from the destination to *b* or *y*. This special case is referred to as local minimum phenomenon and is more likely to occur whenever a routing hole is encountered.

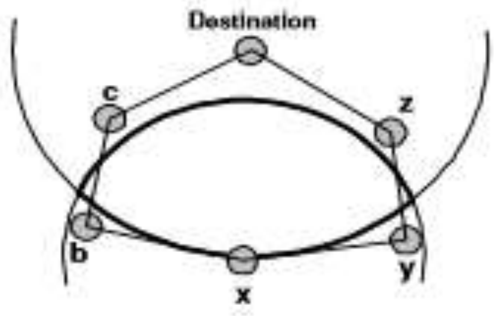


Fig.3 Local minimum phenomenon in greedy forwarding

3 Jamming Holes

An interesting scenario can occur in tracking applications when the object to be tracked is equipped with jammers capable of jamming the radio frequency being used for communication among the sensor nodes [4]. When this happens, nodes will still be able to detect the presence of the object in the area but unable to communicate the occurrence back to the sink because of the communication jamming. This zone of influence centered at the jammer is referred to as jamming hole in this paper. The jamming can be deliberate or unintentional. Unintentional jamming results when one or more of the deployed nodes malfunction and continuously transmits and occupies the wireless channel denying the facility to other neighboring nodes. In deliberate jamming an adversary is trying to impair the functionality of the sensor network by interfering with the communication ability of the sensor nodes. This adversary can be a laptop-class attacker [5]with more resources and capable of affecting a larger area of the sensor network or a mote-class attacker [5] i.e., one of the deployed nodes that has been compromised and is now acting maliciously to create a denial of service condition. Apart from communication jamming, jamming of sensing capabilities is also possible for certain kind of sensor networks e.g. consider the case of a sensor network that relies on acoustic sampling for tracking objects. If the object that is being tracked can introduce random high power acoustic noises, the sensors cannot reliably detect its presence and would be unable to report the existence of the object.

4 Sink/Black Hole/ Worm Hole

Sensor networks are highly susceptible to denial of service attacks due to their inherent characteristics i.e., low computational power, limited memory and communication bandwidth coupled with use of insecure wireless channel. A sink/black hole attack can be easily launched by an adversary node in the sensor network. The malicious node starts advertising very attractive routes to data sink. The neighbor nodes select the malicious node as the next hop for message forwarding considering it a high quality route and propagate this route to other nodes. Almost all traffic is thus attracted to the malicious node that can either drop it, selectively forward it based on some malicious filtering mechanism or change the content of the messages before relaying it. This malicious node has thus formed a sink hole with itself at the center. The sink hole is characterized by intense resource contention among neighboring nodes of the malicious node for the limited bandwidth and channel access [11]. This results in congestion and can accelerate the energy consumption of the nodes involved, leading to the formation of routing holes due to nodes failure. With sink holes forming in a sensor network, several other types of denial of service attacks are then possible [5],[11]. Worm hole is another kind of denial of service attack [12]. Here the malicious nodes, located in different part of the sensor network, create a tunnel among themselves. They start forwarding packets received at one part of the sensor network to the other end of the tunnel using a separate communication radio channel. The receiving malicious node then replays the message in other part of the network. This causes nodes located in different parts of networks to believe that they are neighbors, resulting in incorrect routing convergence.

In this paper we are working mainly on coverage holes.

RELATED WORK

There has been many such related work done on this topic. In this section we highlight the work done in order to detect holes inside the network. I.Khan et al. [2] give a detail description of work done for boundary recognition and hole detection in wireless sensor networks. Fang et al. [4] detects holes inside the network by assuming that nodes are equipped with location awareness devices. The algorithms [10, 26, 27, 28, 29, 30, 35] under this category, use the connectivity information of sensor nodes to detect the boundary of the sensor networks and detect holes inside the wireless sensor network. These algorithms utilize the available topological information and do not make any assumptions about the geographical locations of the nodes. The algorithms [31, 32, 33] proposed under this category identify the nodes, as either inner or boundary nodes, by assuming that the node distribution in the network follows some statistical functions.

An algebraic topological method using homology theory detects single overlay coverage holes without coordinates [4], [5]. Ghrist and Muhammad [4] employed a central control algorithm that requires connectivity information for all nodes in the RoI. For N nodes, the time complexity is $O(N^5)$. For [5], it is $O(HD^2)$, where D is the maximum number of other active nodes that overlap a node's sensing area, and H is the worst-case number of redundant nodes in a large hole, with $H \geq D$. In [5], the complexity does not depend on the overall size of the network, whereas the homology algorithm encounters severe difficulties with dense networks. Additionally, the message forwarding overhead can be impractically large, since the algorithm is centralized.

Funke in [6] presented a heuristic for detecting holes based on the topology of the communication graph. The heuristic computation is not localized as it requires the computation of distance fields over the whole network.

In a more recent paper [7], Funke and Klein described a linear-time algorithm for hole detection. They require that the communication graph follows the unit disk graph model. Compared to the heuristic approach presented in [6], the algorithm does slightly worse. Furthermore, when decreasing the node density, the algorithm breaks down more and more.Wang et al. [22] proposed three different deployment protocols that relocate mobile sensors once coverage holes are detected using Voronoi diagrams. In [23], the authors proposed a scheme called Co-Fi that relocates mobile nodes to replace low energy nodes. Authors in [24] developed three hole-movement strategies for moving an existing big hole in a way that either the total energy consumption is minimized or the power consumption of sensors is balanced.

The incompleteness of previous work motivates our research presented here. Our proposed hole and border detection algorithm is distributed and lightweight, and thus more suited to the energy constrained WSNs. It does not require flooding for gathering the topology information, as is the case in [10] or synchronization among nodes.

PROPOSED METHOD

In our algorithm we propose a mechanisms to detect and heal holes. Our hole detection mechanism deals with holes of various forms and sizes. We try to alert a limited number of nodes surrounding the hole, only those nodes have the task of moving and repairing the hole. And also all the holes are not moved instead the correct path is found and the node reallocation required for that path setup is done.

While designing a hole healing algorithm there are certain important things which should be considered. How to detect the hole, estimate its size, estimate the target location for the reallocation of the node etc.

Our DHD algorithm allows us to discover holes, to compute their characteristics and to discover the network boundary. In a second phase, HEAL performs a local healing where only the nodes located at an appropriate distance from the hole will be involved in the healing process. We define an attractive force that acts from the hole center and attracts the nodes towards the hole center. At the same time, a repulsive force is defined among nodes to minimize the overlapping among them. These forces will be effective in a limited area, which we call the HHA. The proposed algorithms consist of hole detection and hole healing steps. We first discuss how to detect and heal a single hole and then we show how to deal with several holes.

The identification of holes in a wireless sensor network is of primary interest since the breakdown of sensor nodes in a larger area often indicates one of the special events to be monitored by the network in the first place (e.g. outbreak of a fire, destruction by an earthquakes etc.). This task of identifying holes is especially challenging since typical wireless sensor networks consist of lightweight, low capability nodes that are unaware of their geographic location. But there is also a secondary interest in detecting holes in a network: recently routing schemes have been proposed that do not assume knowledge of the geographic location of the network nodes but rather perform routing decisions based on the topology of the communication graph. Holes are salient features of the topology of a communication graph. In the first part of this paper we propose a simple distributed procedure to identify no des near the boundary of the sensor field as well as near hole boundaries. Our hole detection algorithm is based purely on the topology of the communication graph, i.e. the only information available is which nodes can communicate with each other.

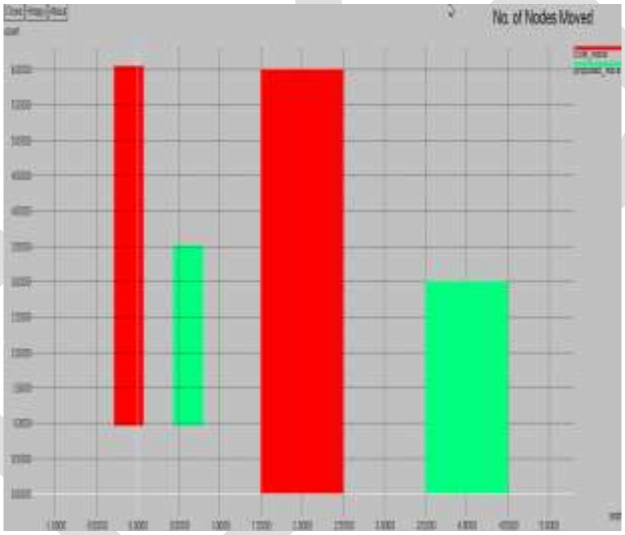
DHD is the algorithm used for the detection of the holes, it can detect multiple number of holes in WSN. DHD is a distributed and localized hole detection algorithm that operates over the Gabriel graph of the network. First we have to access the existence of a hole, which is done by identifying stuck nodes All the nodes that are marked as stuck nodes. From this module we can identify the hole characteristics such as hole position and radius.

SIMULATION AND RESULT

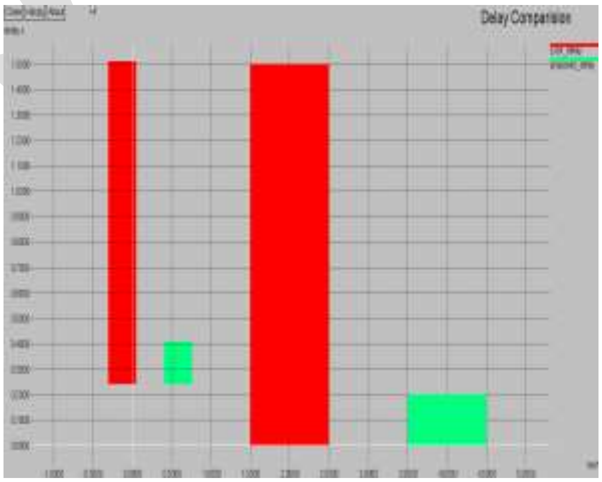
Holes are hindrance for the proper communication in the wireless sensor network. Here in this project these holes are detected automatically and healed by moving the nodes at the boundary of the hole.

We compare some performance characteristics of existing and the proposed systems. The no. of nodes moves and delay characteristics of of the proposed system with the existing technique is compared here. The results are showed in Xgraph

No. of nodes moved: The movement of nodes in the existing and proposed system is compared and examined. The Xgraph figure shown below represents this comparison.



Delay analysis: The figure below shows the delay comparison of the existing and the proposed system. The delay of the proposed system is much less than that of existing system.



CONCLUSION AND FURURE WORK

This paper has proposed and implemented a lightweight and comprehensive two-phase protocol, HEAL, for ensuring area coverage employing a mobile WSN. The protocol uses a distributed DHD to detect holes in the network. . Compared to the existing schemes, DHD has a very low complexity and deals with holes of various forms and sizes despite the nodes distribution and density. By exploiting the virtual forces concept, our approach relocates only the adequate nodes within the shortest time and at the lowest cost.

Through the performance evaluation, we validated HEAL, using different criteria and showed that it detects and heals the holes despite their number or size with less mobility in various situations. The evaluation results demonstrate that HEAL provides a cost-effective and an accurate solution for hole detection and healing in mobile WSNs. In the future, we plan to investigate the interaction between HEAL and the network layer for hole detection and healing. We are currently working on open holes located at the network boundary.

REFERENCES:

[1] N. Ahmed, S.S. Kanhere, and S. Jha, “The Holes Problem in Wireless Sensor Networks: A Survey,” SIGMOBILE Mobile Computing Comm. Rev., vol. 9, no. 2, pp. 4-18, 2005.

[2] B. Wang, Coverage Control in Sensor Networks. Springer, 2010.

[3] B. Kun, T. Kun, G. Naijie, L.D. Wan, and L. Xiaohu, “Topological Hole Detection in Sensor Networks with Cooperative Neighbors,” Proc. Int’l Conf. Systems and Networks Comm. (ICSN ’06), p. 31, 2006.

[4] R. Ghrist and A. Muhammad, “Coverage and Hole-Detection in Sensor Networks via Homology,” Proc. Fourth Int’l Symp. Information Processing in Sensor Networks (IPSN ’05), pp. 254-260, Apr. 2005.

[5] V. De Silva, R. Ghrist, and A. Muhammad, “Blind Swarms for Coverage in 2-D,” Proc. Robotics: Science and Systems, pp. 335-342, June 2005.

[6] F. Stefan, “Topological Hole Detection in Wireless Sensor Networks and its Applications,” Proc. Joint Workshop on Foundations of Mobile Computing, p. 44-53, 2005.

[7] J.W. Cai; P. Yi, Y. Tian, Y.K. Zhou, N. Liu, The Simulation and Comparison of Routing Attacks on DSR Protocol[C], WiCOM 2009, in press.

[8] B. Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks[C]; 5th European Personal Mobile Communications Conference, 2003, 490-495.

[9] A. Patcha; A. Mishra; Collaborative security architecture for black hole attack prevention in mobile ad hoc networks[C]; Radio and Wireless Conference, 2003, 75-78.

[10] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullende

[11] D. Boneh; C. Gentry; B. Lynn; H. Shacham. “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps”. Advances in Cryptology- EUROCRYPT’03: LNCS 2656. Berlin: SpringerVeralg, 2003. 416-432.

[12] D.M. Shila; T. Anjali; Defending selective forwarding attacks in WMNs, IEEE International Conference on Electro/Information Technology, 2008, 96-101.

[13] I.F. Akyildiz; X. Wang (2005). A Survey on Wireless Mesh Networks [J]. IEEE Communications Magazine, 43 (9), 23-30

[14] D.S.J.D. Couto; D. Aguayo; J. Bicket; R. Morris, “A HighThroughput Path Metric for Multi-Hop Wireless routing,” in ACM Mobicom, 2003.

ISSN 2091-2730

[15] J.W. CAI; P. YI, Y. TIAN, Y.K. ZHOU, N. LIU, THE SIMULATION AND COMPARISON OF ROUTING ATTACKS ON DSR PROTOCOL [C], WICOM 2009, IN PRES