International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 2 268 - 272

Reliable Communication using Path Recovering in Wireless Sensor Network

K. MEENA
Student
ME Computer Science Engineering, Anna University
VPMM Engineering College for Womens, VPM Nagar,
Krishnankovil-626190
INDIA
meena93cse@gmail.com
9787637097

K. CHITRA M. Tech
Assistant Professor
Dept of Computer Science Engineering
VPMM Engineering College for Womens, VPM Nagar,
Krishnankovil-626190
INDIA
erchitra.it@gmail.com
9940968777

Abstract:-Sensor technology is one in every of the quick growing technologies within the current scenario. And it's big selection of application additionally. The power of sensors to figure while not being monitored by someone is its distinctive quality. Wireless device network comprise of little sensors that have minimum communicatory and procedure power. Several anomalies square measure gift in WSNs. One such drawback may be a hole. Space barren of any node will be brought up as a hole. This degrades the performance of the full network. It affects the routing capability of the network terribly badly. The formation of holes in an exceedingly WSN is unavoidable thanks to the inner nature of the network. This paper deals with detective work and healing such holes in associate on demand basis.

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

*****

1. Introduction:

A wireless sensing element network consists of tiny sensing element nodes. Every sensing element node is capable of sensing some development, doing some restricted processing and communicating with one another. This tiny sensing element nodes area unit deployed within the target field in massive numbers and that they collaborate to make AN adhoc network capable of coverage the development to a data assortment purpose known as sink or basestation. These networked sensors have many potential in civil further as military applications. ie., they're used for environmental watching, industrial monitoring and that they are used for object chase. Sensing element nodes area unit even used for health connected applications etc.

Several anomalies will occur in wireless sensor networks that impair their desired functions id est., communication and sensing. One such anomaly could be a hole. Destruction of nodes causes holes. Space empty of any node is termed as a hole. Differing types of holes square measure gift particularly coverage holes, routing holes, electronic countermeasures holes, black holes/sink holes etc.

WSN area unit deployed in hostile settingand left unchanged for a comparatively longer period of your time. Now and then a gaggle of sensors fail to hold out the network operations. Such nodes area unit termed as destroyed node. In detector network we have a tendency to come upon a kind of node termed as faulty node. A faulty node may be nodes which supplies result that significantly deviate from the results of itsneighboring nodes. The emergence of holes within the network is inevitable owing to the inner nature of WSNs, random deployment, environmental factors, and external attacks. Thus, an occasion occurring within these holes is neither detected nor reported and, therefore, the most task of the network won't be completed. Thus, it is primeval to supply a self-organizing mechanism to observe and recover holes. This paper seeks the matter of hole detection associate degreed healing in an on demand basis.
Some of the most important reason for nodedestruction and hole creation are:

- Power depletion: every sensing element node is equipped with power battery. Once depleted it's not a straightforward task to recharge the nodes.

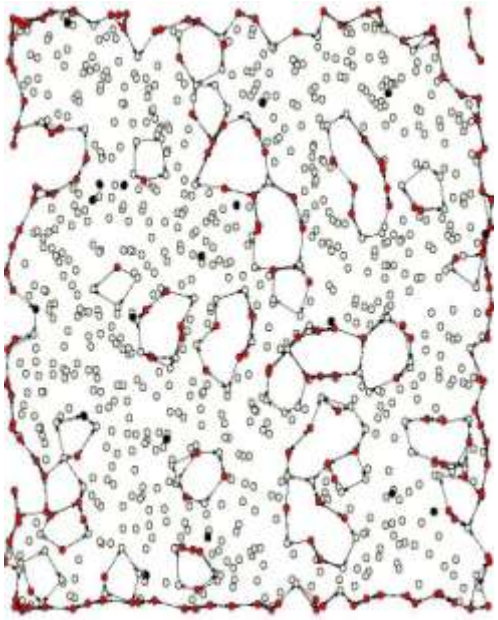
- Physical destruction: Physicaldestruction of nodes owing to some Environmentalreason causes a hole in the network.

- Existence of obstacles: associate degree example for such a scenario could be a sensing element node fell in a very lake wherever its task is to monitor fire. This build the inactive for the aim and a hole is created.

- Lower density regions: Nodes that fall within the lower density region acts as isolated nodes and so they form holes.

2. PROBLEM DEFINITION:

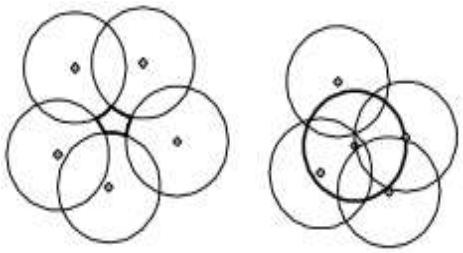
There have been a lot of researches on holedetection downside because it is one amongst the most important problem of wireless sensing element networks. In almost all method the primary methodology id to detect the topology of the network. And it is done by several suggests that. And additionally the kind of the outlet must be known. We formally outline here numerous styles of holes and their characteristics.



2.1 Coverage Holes:

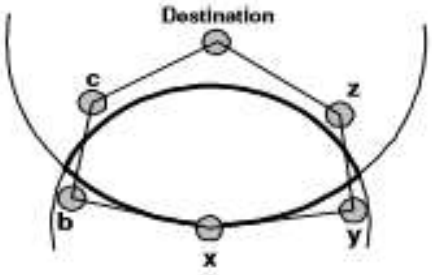
Given a collection of sensors and a target, no coverage hole exists within the target, if every purpose in this target is roofed by at least k sensors, wherever k is that the needed degree of coverage for a selected application (see Fig. 2.1.1). it's pertinent to mention that the coverage hole drawback defined depends on application requirements. Some applications might require a better degree of coverage of a given target for fault tolerance/redundancy or for correct target localization exploitation triangulation-based positioning protocols [7] or trilateration based localization [8].

The sensing coverage of a device node is usually assumed uniform altogether directions and is described by unit disc model (Fig. 1). However, this idealised model relies on false assumption: good and same coverage during a circular disc for all the sensors. Moreover, the coverage not solely depends on the sensing capability of the sensor however additionally on the event characteristics [9] e.g. target detection of military tanks as compared to detection of movement of soldiers depends on the character and characteristics of event furthermore because the sensitivity of the sensors concerned.



2.2 Routing Holes:

A routing hole include a part within the sensor network wherever either nodes don't seem to be available or the out there nodes cannot participate within the actual routing of the information due to varied doable reasons. These holes will be fashioned either attributable to voids in sensor readying or owing to failure of sensor nodes attributable to varied reasons such as wrong, battery depletion or AN external event like fire or structure collapse physically destroying the nodes. Routing holes can even exist attributable to native minimum development typically long-faced in geographic greedy forwarding. Forwarding here relies on destination location. In Fig. 2.2.1, a node x tries to forward the traffic to at least one of its 1-hop neighbor that's geographically nearer to the destination than the node itself. This forwarding process stops once x cannot find any 1-hop neighbor nearer to the destination than itself and also the solely route to destination requires that packet moves quickly farther from the destination to b or y. This special case is spoken as native minimum development and is additional probably to occur whenever a routing hole is encountered.



2.3 Jamming Holes:

An interesting state of affairs will occur in tracking applications once the article to be tracked is supplied with jammers capable of jam the frequency getting used for communication among the device nodes [4]. Once this happens, nodes will still be ready to discover the presence of the object within the space however unable to communicate the prevalence back to the sink due to the communication jamming. This zone of influence focused at the sender is observed as jam hole during this paper. The jam is deliberate or unintentional. Unintentional jamming results once one or a lot of of the deployed nodes malfunction and continuously transmits and occupies the wireless channel denying the power to other neighboring nodes. In deliberate jamming associate degree someone is attempting to impair the practicality of the device network by interfering with the communication ability of the device nodes. This someone is a laptop-class assaulter [5]with a lot of resources and capable of poignant a bigger area of the device network or a mote-class attacker [5] i.e., one amongst the deployed nodes that has been compromised and is currently acting maliciously to make a denial of service condition. Apart from communication jam, jamming of sensing capabilities is additionally potential for certain reasonably device networks e.g. consider the case of a device network that relies on acoustic sampling for chase objects. If the article that's being half-track can introduce random high power acoustic noises, the sensors cannot dependably discover its presence and would be unable to report the existence of the article.

2.4 Sink/Black Hole/ Worm Hole

Sensor networks area unit extremely vulnerable to denial of service attacks because of their inherent characteristics i.e., low computational power, restricted memory and

communication information measure including use of insecure wireless channel. A sink/black hole attack may be simply launched by associate degree human node within the sensor network. The malicious node starts advertising terribly engaging routes to information sink.

The neighbor nodes choose the malicious node because the next hop for message forwarding onsidering it a high quality route and propagate this route to other nodes. most traffic is so attracted to the malicious node which will either drop it, by selection forward it primarily based on some malicious filtering mechanism or change the content of the messages before relaying it. This malicious node has so formed a sink hole with itself at the middle.

The sink hole is characterised by intense resource rivalry among neighboring nodes of the malicious node for the restricted bandwidth and channel entry [11]. This results in congestion and may accelerate the energy consumption of the nodes concerned, leading to the formation of routing holes due to nodes defeat. With sink holes forming in a very detector network, many different types of denial of service attacks area unit then possible [5],[11]. Worm hole is another kind of denial of service attack [12]. Here the malicious nodes, situated in several part of the detector network, produce a tunnel among themselves.

They start forwarding packets received at one a part of the sensing element network to the opposite finish of the tunnel using a different communication radio channel. The receiving malicious node then replays the message in different a part of the network. This causes nodes settled in different elements of networks to believe that they are neighbors, leading to incorrect routing convergence.

3. RELATED WORK

There has been several such connected workdone on this subject. during this section we have a tendency to highlight the work wiped out order to notice holes within the network. I.Khan et al. [2] give a detail description of labor in dire straits boundary recognition and hole detection in wireless device networks. Fang et al. [4] detects holes within the network by assuming that nodes area unit equipped with location awareness devices. The algorithms [10, 26, 27, 28, 29, 30, 35] under this class, use the property information of device nodes to notice the boundary of the device networks and detect holes within the wireless device network. These algorithms utilize the available topological data and don't build any assumptions concerning the geographical locations of the nodes. The algorithms [31, 32, 33] planned beneath this class establish the nodes, as either inner or boundary nodes, by presumptuous that the node distribution within the network follows some applied math functions.

An pure mathematics topological technique victimization homology theory detects single overlay coverage holes while not coordinates [4], [5]. Ghrist and Muhammad [4] used a central management algorithmic rule that needs connectivity data for all nodes in the RoI. For N nodes, the time complexness is O(N5). For [5], it's O(HD2), where D is the maximum variety of different active nodes that overlap a node's sensing space, and H is that the worst-case variety of redundant nodes in an exceedingly giant hole, with $H \geq D$. In [5], the complexness doesn't rely on the size of the network, whereas the similarity algorithmic rule encounters severe difficulties with dense networks. Additionally, the message forwarding overhead will be impractically giant, since the algorithmic rule is centralized.

Funke in [6] given a heuristic for detecting holes supported the topology of the communication graph. The heuristic computation isn't localized because it needs the computation of distance fields over the whole network.

In a more moderen paper [7], Funke and Klein represented a linear-time algorithmic rule for hole detection. They need that the communication graph follows the unit disk graph model. Compared to the heuristic approach conferred in [6], the algorithmic rule does slightly worse. moreover, when decreasing the node density, the algorithmic rule breaks down additional and additional.

Wang et al. [22] planned 3 totally different deployment protocols that relocate mobile sensors once coverage holes square measure detected using Voronoi diagrams. In [23], the authors planned a theme referred to as Co-Fi that relocates mobile nodes to switch lowenergy nodes. Authors in [24] developed three hole-movement methods for moving an existing massive hole in an exceedingly manner that either the total energy consumption is decreased or the power consumption of sensors is balanced.

The integrity of previous work motivates our analysis given here. Our proposed hole and border detection algorithm is distributed and light-weight, and so additional suited to the energy constrained WSNs. It doesn't need flooding for gathering the topology information, as is that the case in [10] or synchronization among nodes.

4. PROPOSED METHOD:

In our formula we have a tendency to propose a mechanismsto discover and heal holes. Our hole detection mechanism deals with holes of various forms and sizes. we have a tendency to try and alert a limited variety of nodes close the hole, solely those nodes have the task of moving and repairing the opening. And also all the holes aren't moved instead the correct path is found and also the node reallocation needed for that path setup is done.

While coming up with a hole healing algorithmic program there square measure bound vital things that should be thought of. a way to notice the hole, estimate its size, estimate the target location for the reallocation of the node etc.

Our DHD algorithmic program permits U.S.A. to find holes, to reason their characteristics and to discover the network boundary. In a second section, HEAL performs a

neighborhood healing wherever solely the nodes situated at Associate in Nursing appropriate distance from the outlet are involved within the healing method. We define an attractive force that acts from the outlet center and attracts the nodes towards the hole center. At identical time, a repulsive force is defined among nodes to attenuate the overlapping among them. These forces will be effective in a very restricted space, which we decision the HHA. The planned algorithms consist of hole detection and hole healing steps. we tend to first discuss a way to discover and heal one hole then we tend to show however to agitate many holes.

The identification of holes during a wirelesssensor network is of primary interest since the breakdown of sensing element nodes during a larger area usually indicates one in all the special events to be monitored by the network in the first place (e.g. irruption of a hearth, destruction by AN earthquakes etc.). This task of distinguishing holes is very challenging since typical wireless sensing element networks comprises light-weight, low capability nodes that square measure unaware of their geographic location. however there's additionally a secondary interest in detection holes during a network: recently routing schemes have been projected that don't assume knowledge of the geographic location of the network nodes however rather perform routing selections supported the topology of the communication graph. Holes are salient options of the topology of a communication graph. within the initial a part of this paper we have a tendency to propose a straightforward distributed procedure to spot no des close to the boundary of the sensing element field likewise as near hole boundaries. Our hole detection formula is predicated strictly on the topologyof the communication graph, i.e. the only information accessible is that nodes will communicate with one another.

DHD is that the rule used for thedetection of the holes, it will notice multiple range of holes in WSN. DHD is a distributed and localized hole detection rule that operates over the Gabriel graph of the network. First we have to access the existence of a hole, which is completed by distinctive stuck nodes All the nodes that area unit marked as stuck nodes. From this module we will determine the hole characteristics like hole position and radius.

Border detection formula is distributed and light weight. The boundary nodes square measure detcted by that square measure struct nodes, struck nodes square measure those nodes that cannot transmit packets additional to ensuing hop neighbours.These nodes can launch the hole discovery and therefore the healing methodeven if these nodes are literally not stuck nodes.

The formation of holes impact the wholepresentation of wireless detector networks. They give rise to variety of coverage and routing issues.

guaranteeing information reliability: For accurate results the sphere ought to be completely coated with device nodes. Formation of holes have an effect on data dependability.

 Virtual co-ordinate ssystem: The detection of holes will facilitate in computing virtual co-ordinates. Virtual co-ordinate system assigns virtual co-ordinate to nodes within the network with relevance some chosen reference nodes. Holes would possibly hinder the shortest path between the nodes. Once holes area unit detected the virtual co-ordinates assignment gets straightforward and thus geographical routing improves.

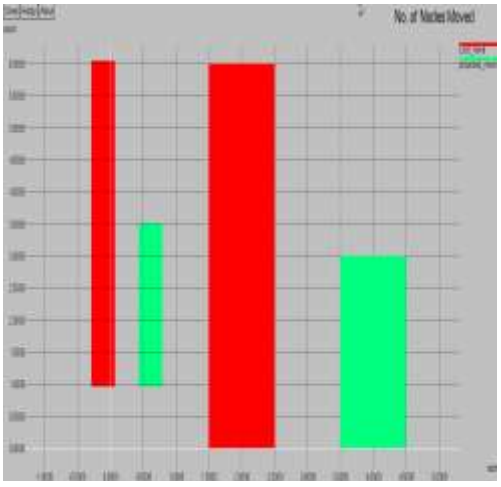
We exploit here nodes shifting facilities to heal detected holes. Our relocation algorithmic rule is totally distributed and it's supported the concept of virtual forces. To heal the discovered hole we tend to outline a lovely force that acts from the opening center and attracts the nodes towards this center. Similarly, a force is outlined among nodes to reduce the overlapping in between. we tend to outline the HHA within which the forces are effective. this permits a eighborhood healing where solely the nodes settled at AN appropriate distance from the opening can be concerned within the healing method.

5. SIMULATION AND RESULT

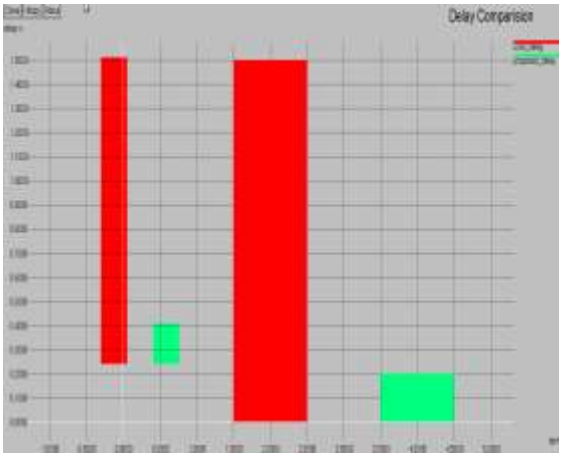
Holes square measure hindrance for the correct communication with in the wireless device network. Here during this project these holes square measure detected mechanically and healed by moving the nodes at the boundary of the opening.

We measure some performance characteristics of existing and therefore the proposed systems. The no. of nodes moves and delay characteristics of ofthe projected system with the prevailing technique is compared here. The results area unit showed in Xgraph

No. of nodes moved:
The movement of nodes within the existing andproposed system is compared and examined. The Xgraph**figure** 5.1 shown below represents this comparison.



Delay analysis:
The figure below shows the delay comparison of the present and therefore the proposed system. The delay of the proposed system is far but that of existing system.



6. CONCLUSION:

This paper has planned and enforceda lightweight and comprehensive two-phase protocol, HEAL, for guaranteeing spacecoverage using a mobile WSN. Theprotocol uses a distributed DHD to noticeholes within the network.

Compared to theexisting schemes, DHD encompasses a terribly lowcomplexity and deals with holes of assortedforms and sizes despite the nodesdistribution and density. By exploiting theeffective forces thought, our approachrelocates solely the adequate nodes amongthe shortest time and at rock bottom price.

Through the performance analysis, wevalidated HEAL, victimisation completely different criteria and showed that it detects and heals the holes despite their variety or size with less mobility in varied things. The evaluation results demonstrate that HEAL provides an economical associate degreed an correct solution for hole detection and healing in mobile WSNs. within the future, we plan to investigate the interaction between HEAL and the network layer for hole detection and healing. we tend to area unit presently engaged on open holes set at the network boundary.

7. 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.
[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 press