Distributed Algorithm for Fast Detecting the Failure Nodes Chronicles

VENKAT RAO KOMMURI[#1], NAGUL SHAIK[#2], ANIL KUMAR DASARI[#3]

[#1, 2] Department of Computer Science Engineering, Nimra College (NIST)

***Abstract*— with the fast transferring the data some of the nodes will not working while transferring the information that is called the cut. To avoid this problem one of the algorithm is proposed and we have to demonstrate that algorithm Cut Detection algorithm in that algorithm enables every node of a wireless sensor network to detect Disconnected from Source events if they occur. It enables a subset of nodes that experience CCOS events to detect them and estimate the approximate location of the cut in the form of a list of active nodes that lie at the boundary of the cut. Defined with respect to a specially designated source node. The algorithm is based effectively with large classes of graphs of varying size and structure, without requiring changes in the parameters. For certain scenarios, the algorithm is assured to detect connection and disconnection to the source node without error. A key strength of the DCD algorithm is that the convergence rate of the underlying iterative scheme is quite fast and independent of the size and structure of the network, which makes detection using this algorithm quite fast.**

Keywords **-** Application, Cut, Detection, Electrical, Fast, Network, Nodes, Parameter, Research, Wireless network

I. INTRODUCTION

A sensor network typically consists of hundreds, or even thousands, of small, low-cost nodes distributed over a wide area. The nodes are expected to function in an unsupervised fashion even if new nodes are added or old nodes disappear (e.g., due to power loss or accidental damage). While some networks include central location for data collection, many operate in an entirely distributed manner, allowing the operators to retrieve aggregated data from any of the nodes in the network. Furthermore, data collection may only occur at irregular intervals. For example, many military applications strive to avoid any centralized and fixed points of failure. In fact, node failure is expected to be quite common due to the typically limited energy budget of the nodes that are powered by small batteries. Failure of a set of nodes will reduce the number of multi hop paths in the network.

Disadvantages:

Unsuitable for dynamic network reconfiguration. Single path routing approach.

Proposed System:

Monitoring large high spatial and temporal resolution of the networks and failure occur at the set of nodes will reduce the number of hop paths in the network. Such failures can cause a subset of nodes – that have not failed to become disconnected from the rest, resulting in a "cut". Two nodes are said to be disconnected if there is no path between them. We consider the problem of detecting cuts by the nodes of a wireless network. We consider the problem of detecting cuts in wireless network. We assume that there is a specially designated node in the network, which we call the source node. The source node is the base station that serves as an interface between the network and its users. Since a cut may or may not separate a node from the source node, we distinguish between two distinct outcomes of a cut for a particular node. When a node *u* is disconnected from the source, we say that a Disconnected from Source event has occurred for *u*. When a cut occurs in the network that does not separate a node *u* from the source node, we say that Connected, but a Cut Occurred Somewhere CCOS event has occurred for *u*. By cut detection we mean 1) detection by each node when cut occurs, and 2) detection of CCOS events by the nodes close to a cut, and the approximate location of the cut. We mean the location of one or more active nodes that lie at the boundary of the cut and that are connected to the source. Nodes that detect the occurrence and approximate locations of the cuts can then alert the source node or the base station.

Advantages:

Local communication between neighboring nodes, and is robust to temporary communication failure between node pairs

II. BACKGROUND

The great number of nodes that in general compose a WSN provides good results. Neighbor nodes can monitor each others' behaviors and when a problem is detected, such as a node crash (a situation in which a node is permanently out of order), one or some of its neighbors can assume the tasks that were previously executed by the faulty node. However, the assumption of access to redundant nodes is a necessary condition for the success of this approach. In the lifespan of a WSN, it is probable that the node density eventually decreases and fewer nodes may then be able to count on the initial redundancy, due to the failure of a number of the previously available nodes in the vicinity. Moreover, there are situations in which it is not desired to deploy a WSN with too many redundant nodes, and then the overlap between the sensed areas are smaller, which reduces the robustness of design approaches that assume redundancy for it to work. An example of such situations in which redundancy based on a unnecessary high density of nodes is not desired is the deployment in an area in which the nodes should be as invisible as possible, e.g. for secrecy, and in which a high concentration of them would offer an opportunity to easily detect their presence.
The node status in WSNs can be divided into two types normal and faulty. Faulty in turn can be "permanent" or "static". The so-called "permanent" means failed nodes will remain faulty until they are replaced, and the so-called "static" means new faults will not generated during fault detection. In, node faults of WSNs can be divided into two categories: hard and soft. The so-called "hard fault" is when a sensor node cannot communicate with other nodes because of the failure of a certain module (e.g., communication failure due to the failure of the communication module, energy depletion of node, being out of the communication range of entire mobile network because of the nodes' moving and so on). The so-called "soft fault" means the failed nodes can continue to work and communicate with other nodes (hardware and software of communication module are normal), but the data sensed or transmitted is not correct. The purpose of this paper is to study the needs for detecting the failure nodes, in the above mentioned situations of WSN.

III. PROPOSED SYSTEM ARCHITECTURE

The algorithm allows each node to detect DOS. The algorithm we propose is distributed and asynchronous: it involves only local communication between neighboring nodes, and is robust to temporary communication failure between node pairs.

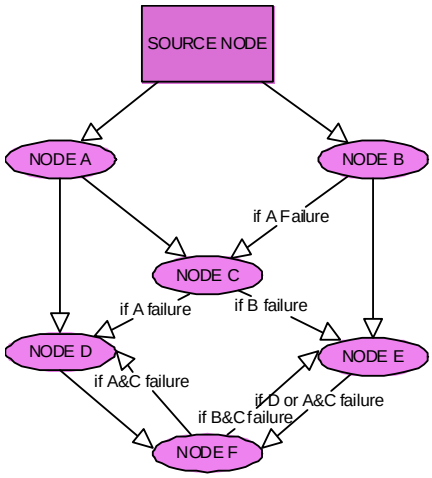


Fig. 1.usecase Diagram

A key component of the DCD algorithm is a distributed iterative computational step through which the nodes compute their (fictitious) electrical potentials. The convergence rate of the computation is independent of the size and structure of the network.

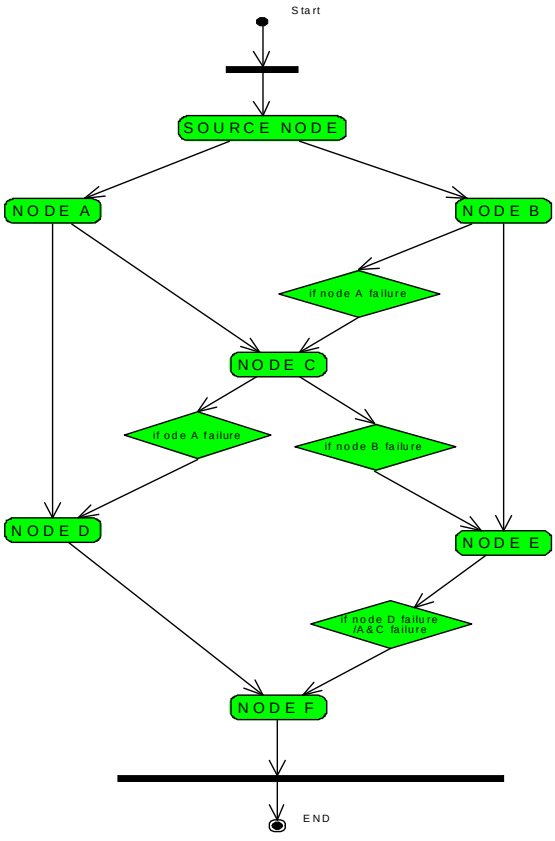


Fig 2 Activity Diagram

In the above diagrams that will any failures of the node then it will be changed the root to the other to pass the information with out having the lost of information or the delay of the information or delay of the message if the node fails. The information can pass the other root. The algorithm for detecting CCOS (Connected, but a Cut Occurred Somewhere) events on finding a short path, and is partially inspired by the jamming detection algorithm proposed in The method utilizes node states to assign the task of hole-detection to the most appropriate nodes. When a node detects a large change in its local state as well as failure of one or more of its neighbors, and both of these events occur within a (predetermined) small time interval.

IV. IMPLEMENTATION

In this paper our proposed method consists following modules.

Distributed cut Detection:

Distributed iterative computational step through which the nodes compute their electrical potentials. That will shows the where the cut will appear and solve.

Cut:

A wireless sensor network can get separated into multiple connected components due to the failure of some of its nodes which is called a “cut.”

Source node:

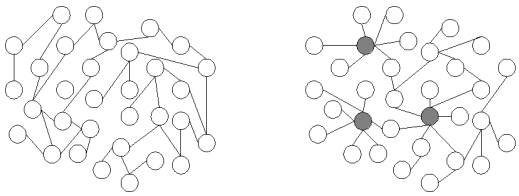
We consider the problem of detecting cuts by the nodes of a wireless network. We assume that there is a especially designated node in the network, which we call the source node. The source node may be a base station interface between the network and its users. Since a cut may or may not separate a node from the source node, we distinguish between two distinct outcomes of a cut for a particular node.

Network separation:

Some nodes may separate from the network, that results the separated nodes can’t receive the data from the source node.

V. RESULT ANALYSIS

Experimental Evaluation We evaluated that the detecting the cut for the failure nodes and working with high utility of the sensing the networks. Recall that the CCOS detection part of the algorithm is applicable to 2D networks, so it was only tested on networks. And the working of the CCOS detection rectifying will be observed by help of DCD algorithm. The experiments were executed on a Windows XP Professional machine with 3 GHz CPU and 2 GB of main memory, running Windows XP Professional. All algorithms were implemented in Java and Oracle 10g was used as the database. The below figures shows the difference between the scale free network and random network.



(a) Random network (b) Scale-free network

VI. CONCLUSION

Detecting cuts by the remaining nodes of a wireless sensor network. Algorithm that allows every node to detect when the connectivity to a specially designated node has been lost, and one or more nodes (that are connected to the special node after the cut) to detect the occurrence of the cut. The algorithm is distributed and asynchronous: every node needs to communicate with only those nodes that are within its communication range. The algorithm is based on the iterative computation of a fictitious electrical potential of the nodes.

REFERENCES

[1] X. Cao and X. Guo, "Partially Observable Markov Decision Processes With Reward Information: Basic Ideas and Models," IEEE Transactions on Automatic Control, vol.52, no.4, Apr. 2007, pp.677-681

[2] J. Lessmann, T. Heimfarth, P. Janacik, “ShoX: An Easy to Use Simulation Platform for Wireless Networks,” Proc. of 10th International Conference on Computer Modeling and Simulation, 2008, pp. 410-415.

[3] A.T. Erman, L. Hoesel and P. Havinga, “Enabling Mobility in Heterogeneous Wireless

Sensor Networks Cooperating with UAVs for Mission-Critical Management," IEEE Wireless Communications, vol.
15, is. 6, 2008, pp. 38-46.

[4] M. Hauspie, J. Carle, and D. Simplot, "Partition Detection in Mobile Ad-Hoc Networks," Proc. Second Mediterranean Workshop Ad-Hoc Networks, pp. 25-27, 2003.

[5] J. NewsomeE, . Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of lEEE Conference on Information Processing in Sensor Networks (IPSN),* Apr. 2004.

[6] A.D. Wood, J.A. Stankovic, and S.H. Son, "Jam: A Jammed-Area Mapping Service for Sensor Networks," Proc. IEEE Real Time Systems Symp., 2003.

[7] M.A. Pasha, S. Derrien and O. Sentieys, "Toward ultra low-power hardware specialization of a Wireless Sensor Network node," Proc. IEEE 13th International Multitopic Conference, 2009. INMIC 2009, Dec. 2009, pp.1-6.

[8] S. Ratnasamy, B. Karp, L. Yin, E Yu, D. Estrin, R. Govindan, and S. Shenker. GHT: A geographic hash table for data-centric storage. In *Proceedings of ACM International Workshop on Wireless Sensor Networks an Applications (WSNA),* Sept. 2002

K VENKAT RAO is a student of Computer Science from **NIMRA COLLEGE OF INFORMATION AND SCIENCE AND TECHNOLOGY,** nimra nagar jupudi, presently pursuing M.tech from this college. He received M.C.A from Nagarjuna University in the year 2011. His research interested in Networks.

SHAIK NAGUL received his M.tech in computer science Engineering from **Acharya Nagarjuna University** in 2011.He is a good researcher. Who has presented nearly 5 various International journals and he is working as Asst.Professor & HOD in Dept. of Computer Science and Engineering. He is a good researcher in Networks and Neural networks.

ANILKUMAR DASARI received his M.tech in computer science Engineering from **JNTUK** and he published 4 International journals in various publications. He is a good researcher who has worked mostly on networks and networks security.