International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

CCOS Detection and Security in Wireless Sensor Network

Shanmugam Shoba M[1], Bhuvitha R[2], Sandeep R[3], Sameer S Nayak[4], Shailaja C[5]
[1,2,3,4,5]*Information Science Engineering,New Horizon College of Engineering*

Abstract-A wireless sensor network can get disunited into multiple connected components due to the failure of some of its nodes, which is called a "cut". Here consider the quandary of detecting cuts by the remaining nodes of a wireless sensor network. Here propose an algorithm that sanctions (i) every node to detect when the connectivity to a specially designated node has been lost, and (ii) 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 predicated on the iterative computation of a fictitious "electrical potential" of the nodes. The convergence rate of the underlying iterative scheme is independent of the size and structure of the network. All cut nodes information is been updated and engendered into a log file of system and filtered log records of cut nodes are maintained.
Keywords-wireless sensor network, node, cut, electrical potential, distributed, asynchronous.

I. INTRODUCTION

Wireless sensor networks (WSNs) are a promising technology for monitoring sizably voluminous regions at high spatial and temporal resolution. In fact, node failure is expected to be quite prevalent due to the typically inhibited energy budget of the nodes that are powered by diminutive batteries. Failure of a set of nodes will reduce the number of multi-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 verbalized to be disconnected if there is no path between them. Wireless sensor networks (WSNs), consisting of sizably voluminous numbers of low-cost and low-power wireless nodes, have recently been employed in many applications: disaster replication, military surveillance, and medical care among others. The intrinsical nature of WSNs such as unattended operation, battery-powered nodes, and astringent environments pose major challenges. One of the challenges is to ascertain that the network is connected. The connectivity of the network can facilely be disrupted due to capricious wireless channels, early depletion of node's energy, and physical tampering by bellicose users. Network disconnection, typically referred as a network cut, may cause a number of quandaries.

II. LITERATURE SURVEY

In paper [1], Nisheeth Shrivastava propose a low overhead scheme for detecting a network partition or cut in a sensor network. Consider a set S of n sensors, which are modeled as points in the two-dimensional plane. An adversary can make a linear cut through the sensor network, incapacitating all the sensors on one side of the line; the base station is surmised to lie on the other (safe) side. Formally, given a line L, let L−and L+ denote the two half-planes defined by L, and let L−(S) and L+(S) denote the subset of sensors that lie in these half-planes. Alternatively, the adversary can disrupt the communication so that sensors on one side of the line cannot communicate with sensors on the other side, including the base station. Here it is call a linear cut an ε-cut if at least ε fraction of the sensors are cut off, where $0 < \varepsilon < 1$ is a userspecified parameter. The Distributed Source Disseverment Detection (DSSD) algorithm proposed is not constrained to ε-linear cuts; it can detect cuts that disunite the network into multiple components of arbitrary shapes. Furthermore, the DSSD algorithms not restricted to networks deployed in 2D, it does not require deploying sentinel nodes, and it sanctions every node to detect if a cut occurs. The DSSD algorithm involves only most proximate neighbour communication, which eliminates the desideratum of routing messages to the source node. This feature makes the algorithm applicable to mobile nodes as well. The cut detection quandary was first considered in a wired network [2]. Kleinberg et al. [2] introduce the concept of (ε, k) -cut, which is defined as a network disseverment into two sets of nodes, namely (1 − ε)n nodes and εn nodes (n refers to the total number of nodes), caused by k independently incapacitated edges. A set of agents, denoted by a set D, is strategically deployed in the network to detect the (ε, k)-cut. Each agent exchanges a control packet with other agents periodically. A cut is surmised to be present if the control message loss exceeds some threshold. Ritter et al. [3] proposed a cut detection algorithm where a sink node broadcasts an alive message. A cut is detected by border nodes, which are located on the border of network, if these nodes fail to receive the alive message more than a certain number of times. In paper [4], Myounggyu Won proposes solutions for a more general cut detection quandary – the destination-predicated cut detection quandary. Unlike the traditional cut detection quandary, Here an endeavor to find a network cut between a sender and any node in a set of given destinations. Point-to-Point Cut Detection protocol (P2P-CD) is utilized. P2P-CD sanctions source node to identify a cut with deference to any destination node. In this protocol, the boundary of a cut is compactly represented as a set of linear segments. The compact representation of a cut sanctions the information on subsisting cuts to be efficiently distributed throughout the network with diminutive overheads. A source node, utilizing the distributed information, locally determines whether any potential destination is reachable.

III. CONCLUSION

In this report, a distributed algorithm is proposed to detect cuts, denominated the Distributed Cut Detection (DCD) algorithm. The algorithm sanctions each node to detect DOS events and a subset of nodes to detect CCOS events. The algorithm propose here is distributed and asynchronous: it involves only local communication between neighboring nodes, and it can be robust to ad interim communication failure between node pairs. A key component of the DCD algorithm is a distributed iterative computational step through which the nodes compute their electrical potentials. The convergence rate of the computation is independent of the size and structure of the network. The DCD algorithm is utilized for every node of a wireless sensor network to detect Disconnected from Source events if they occur. Second, it is withal utilized for 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/aperture. The DOS and CCOS events are defined with deference to a specially designated source node. The algorithm is predicated on conceptions from electrical network theory and parallel iterative solution of linear equations. All cut nodes information is been updated and engendered into a log file of system and filtered log records of cut nodes are maintained.

REFERENCES

[1] N. Shrivastava, S. Suri, and C. Toth, "Detecting cuts in sensor networks," ACM Transactions on Sensor Networks, vol. 4, no. 2, pp. 1–25, 2008.
[2] J. Kleinberg, M. Sandler, and A. Slivkins, "Network failure detection and graph connectivity," in Proc. of ACM SODA , 2004.
[3] H. Ritter, R. Winter, and J. Schiller, " Partition detection system for mobile ad-hoc networks," in Proc. of IEEE SECON, 2004.
[4]Myounggyu Won and Radu Stoleru,"Destination-based Cut Detection in Wireless Sensor Networks", 2011 Ninth IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.