International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 1 Issue: 10 767 – 770

A new Approach on Survey of Cut Detection in Wireless Sensor Networks

KAMINENI.B.T.SUNDARI[1], MUKTHARBABA SHAIK [2], S P CHOUDARY KURRA[3]
Asst.Professor[1, 2, 3],
Avanthi Institute of Engineering & Technology, Hyderabad

***Abstract*— 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". In this article we consider the problem of detecting cuts by the remaining nodes of a wireless sensor network. We propose an algorithm that allows (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 based 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. Wireless Sensor Networks (WSNs) consist of thousands of tiny nodes having the capability of sensing, computation, and wireless communications. Wireless sensor network can suffer partition problem in the network which is called a cut. So a single topology of the network breaks into two or more parts. Here we discuss several cut detection techniques to detect the cuts in WSN.**

*****

I. EXISTING SYSTEM

Wireless sensor network is composed of a powerful base station and a set of low-end sensor nodes. Base station and sensor nodes have wireless capabilities and communicate through a wireless, multihop, ad-hoc network. Wireless sensor networks (WSN) have emerged as an important new technology for instrumenting and observ ing the physical world. WIRELESS sensor networks (WSNs) are a capable scenario for sensing large areas at high spatial and positive resolution. However, the tiny size and low cost of the processing machines that makes them attractive for large deployment also causes the loss of low operational reliability. Wireless sensor networks (WSN) have emerged as an important new technology for instrumenting and observing the physical world. The basic building block of these networks is a tiny microprocessor integra ted with one or more MEMS (micro electromechanical system) sensors, actuators, and a wireless transceiver. A WSN is usually collection of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the ability to gather data and route data back to a base station (BS). A sensor has four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit.

Wireless Multimedia Sensor Networks (WMSNs) has many challenges such as nature of wireless media and multimedia information transmission. Consequently traditional mechanisms for network layers are no longer acceptable or applicable for these networks. Wireless sensor network can get separated into multiple connected components due to the failure of some of its nodes, which is called a "cut". Existing cut detection system deployed only for wired networks.

Disadvantages

1. Unsuitable for dynamic network reconfiguration.
2. Single path routing approach.

II. PROPOSED SYSTEM

Wireless sensor networks (WSNs) are a promising technology for monitoring large regions at high spatial and temporal resolution .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 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 assume that there is a specially designated node in the network, which we call the source nodeSince 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 DOS (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 CCOS (Connected, but a Cut Occurred Somewhere) event has occurred for u. By cut detection we mean (i) detection by each node of a DOS event when it occurs, and (ii) detection of CCOS events by the nodes close to a cut, and the approximate location of the cut. In this article we propose a distributed algorithm to detect cuts, named the Distributed Cut Detection (DCD) algorithm. The algorithm allows each node to detect DOS events and a subset of nodes to detect CCOS events. 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 The convergence rate of the computation is independent of the size and structure of the network.

III. MODULE DESCRIPTION

DISTRIBUTED CUT DETECTION

The algorithm allows each node to detect DOS events and a subset of nodes to detect CCOS events. 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. 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.

CUTS IN WIRELESS SENSOR NETWORKS

ONE of the unique challenges in mobile adhoc networking environments is the phenomenon of network partitioning, which is the breakdown of a connected network topology into two or more separate, disconnected topologies.[3] Similarly sensors become fail for several reasons and the network may breaks into two or more divided partitions so can say that when a number of sensor fails so the topology changes. A node may fail due to a variety of conditions such as mechanical or electrical problems, environmental degradation, and battery reduction. In fact, node failure is expected to be quite common anomaly due to the typically limited energy storage of the nodes that are powered by small batteries. Failure of a set of nodes will reduce the number of multihop paths in the network. Such failures can cause a subset of nodes that have not failed to become disconnected from the rest of the network, resulting in a partition of the network also called a "cut". Two nodes are said to be disconnected if there is no path between them. And As we know that sensors has Disconnectivity from the network is normally referred as a partition of the network of cut in the wireless sensor network, which arise many problems like unreliability ,data loss, performance degradation. Because of cutsin wireless sensor network many problems may arise like a wired network means data loss problem arises, means data reach in a disconnected route.

PROBLEMS DUE TO CUTS

As mentioned above if any node breaks down then the network is separated into different parts so the topology of the network changes but still network works. But because partition affects reliability, data loss, QOS of the network, efficiency, data processing speed. Because if any data passes unfortunately in a wrong route so data loss occurs this also shows unreliability of the network.

SOURCE NODE:

We consider the problem of detecting cuts by the nodes of a wireless network. We assume that there is a specially designated node in the network, which we call the *source node*. The source node may be a 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.

A. Cuts in Sensor Networks

Consider a set S of n sensors, which are modeled as points in the two-dimensional plane. (More generally, we can assume that the sensors lie on a surface or terrain that is topologically equivalent to the plane.) An adversary can make a linear cut through the sensor network, disabling all the sensors on one side of the line; the base station is assumed 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. We will adopt the convention that the linear cut induced by L disables all the sensors in L−(S). 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. These two formulations are equivalent for our purpose. There are other natural forms of cuts, such as circular cuts, rectangular cuts, polygonal cuts.

We call a linear cut an "-cut if at least " fraction of the sensors are cut off, where 0 < € < 1 is a user-specified parameter. Formally, L is an €-cut if |L−(S)| ¸ "|S|. Our primary focus in this paper is to develop a low-overhead scheme for detecting €-cuts in sensor networks.

Our scheme for detecting €-cuts will choose a small subset of sensors, which act as sentinels. Each sentinel will communicate with the base station at a regular time interval. We assume that the base station is not attacked, and it always lies in the safe halfplane L+. A communication failure from a sentinel is taken to mean that the sentinel has been cut off. Our problem now becomes: can one choose a small number of sensor nodes as sentinels so that (1) every €-cut can be detected based solely on the live/dead status of sentinels, and (2) the algorithm does not report false positives. Suppose we show a collection of 1000 sensor nodes, distributed uniformly at random, and its sentinel set for " = 0.05. Before describing our results, we first briefly discuss why we chose €-cuts as our definition, why avoiding false positives is challenging, and why the detection scheme requires an approximation slack.

B. €-Cuts

The €-cuts are motivated both by practical and theoretical concerns. It makes practical sense to treat failures as significant only when a fraction of the network is cut. It may be tempting to ask for schemes that detect failure of a fixed (user-specified) number of sensors, regardless of the network size. However, no efficient and scalable solution is theoretically possible in this case, as the following simple example shows. Imagine n sensors arranged in a circle, and suppose we want to detect cuts of size m. Then, at least one sensor for every m consecutive sensors must be chosen as a sentinel, which scales very poorly with the network size.

C. False Positives

By monitoring sufficiently many randomly chosen sensors, one can detect all €-cuts with high probability. For instance, a random sample of size O(1/€log 1/ δ €) is sufficient to catch any "-cut with probability at least 1 − δ[21], [22]. The algorithm simply declares an €-cut whenever at least one of the chosen sensors fails. Unfortunately, this simple scheme suffers from the false positives problem. Many cuts reported by this algorithm, however, are false positives, where the size of the failed network can be arbitrarily smaller than €n. Indeed, if one of the random samples happens to lie on the boundary of the sensor field, then it can cause an alarm even if a single sensor is cut off. A more sophisticated form of sampling can effectively eliminate false positives, but at the expense of a very large number of sentinels. In particular, the concept of €-approximation can be used to distinguish between all cuts larger than €n and those smaller than, say, 1/2€n. But an €-approximation requires £(1/€2 log 1 δ) sentinel nodes. A simple calculation, including the actual constants involved, however, shows that even for modest values of €= 0.1 and δ = 0.05, the size of the sentinel set is at least 10,000! Thus, random sampling based schemes are infeasible, due to false positives or due to unscalably large size.

Lemma : In an arrangement of n lines in the plane, there is always a level of size at most 6n between the levels 5/6€n and €n. Similarly, there is always a level of size at most 4n between levels 2/3€n and 1/2€n.

Proof: The total complexity of the first €n levels is at most €n2. Clearly, this is also an upper bound on the total complexity of the 1/6€n +1 levels between levels €n and 5/6€n. By the pigeon hole principle, at least one of these levels must have size at most €n2/(1/6€n+1)6n. An analogous argument shows that there is a level of size at most 4n between levels 2/3€n and 1/2€n

We can now complete the proof of Theorem.

Proof: Consider an arrangement of n lines in the plane. Choose a and b such that 1 /2€n< a< 2/3€n< b<€n, and the size of the a level is at most 4n and the size of the b-level is at most 6n; such a and b exist by the preceding lemma. The total size of these two levels is at most 10n, and (b − a + 1) ¸ 1/6€n. By Lemma, we conclude that there is a zig-zag path of size O(1€) between levels a and b. This zig-zag path is clearly a separator between the €n and the 1/2€n levels.

The constant factors in Theorem are quite loose. Our primary goal is simply of prove the asymptotic result that sentinel sets of size O(1 €) exist. Our simulations show that in practice the sentinels sets are significantly smaller than the worst-case bound would indicate.

Detecting €-cuts from a signature

The €n sensors that are cut off may lie either below or above the line. We, therefore, compute two separators, one to detect separation of points below the cutting line, and the other to detect separation above the line. In order to avoid unnecessary replication, we describe our scheme for the lower separator, with the understanding that the complete construction involves a symmetric application of the algorithm for the other case as well.

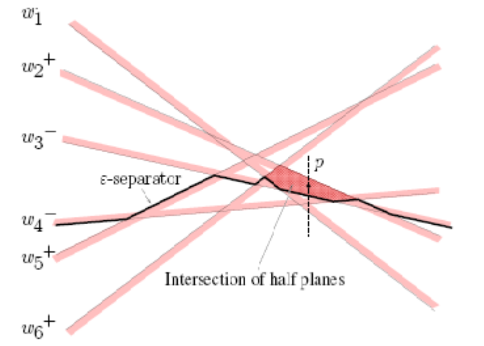

Fig. The intersection of the half-planes determined by the sentinel lines is a cell of the arrangement.

NETWORK SEPERATION:

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". Because of cut, some nodes may separated from the network, that results the separated nodes can't receive the data from the source node.

CONCLUSION

In this article we discuss WSN cuts and existing cut detection schemes in WSN. Wireless Sensor Networks (WSNs) often suffer from disrupted connectivity caused by its numerous aspects such as limited battery power of a node and unattended operation vulnerable to violent interfering. And this loosing connectivity is often referred as a network cut sometimes. In this paper, we studied several schemes of detecting cuts and we conclude by stating that cuts in WSN are a big problem which may introduce some unreliability in the network. So it is necessary to identify and detect cuts in WSN. To the best of our knowledge and based on our studies and reviews, no useful and efficientcut detection scheme has been proposed and implemented so far.

About the authors:

KAMINENI.B.T.SUNDARI Working as Assoc.Professor in CSE Departement at Avanthi Institute of Engineering & Technology, She has 10 years of experience in teaching field. She has a vast experience in research work.

MUKTHARBABA SHAIK working as Asst.Professor in CSE Department at Avanthi Institute of Engineering & Technology. He has 2 years of experience in teaching field.

S P CHOUDARY KURRA working as Asst.Professor in CSE Department at Avanthi Institute of Engineering & Technology. He has 1 year of experience in teaching field.