IJETAE
EXPLORING RESEARCH AND INNOVATIONS

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013)

Wireless Sensor Network Cuts: A Survey

Gajendra Singh Chandel[1], Rakesh Shrivastava[2]
[1]Asst Professor, [2]Student Mtech (IT), SSSIST Sehore (M.P)

***Abstract*— This document gives formatting guidelines for authors preparing papers for publication in the International Journal of Emerging Technology and Advanced Engineering The authors must follow the instructions given in the document for the papers to be published 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.**

***Keywords*— WSN-wireless sensor networks, MEMS-micro-electromechanical system, QOS-quality of service p2p-point to point.**

I. INTRODUCTION

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, multi-hop, ad-hoc network.[3]Wireless sensor networks (WSN) have emerged as an important new technology for instrumenting and observing 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[1].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 integrated with one or more MEMS (micro-electromechanical system) sensors, actuators, and a wireless transceiver.[2] 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 [5]. Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. Wireless sensor network contains large number of nodes and each node may be very close to each neighbor. Since WSN should use multihop techniques because it consume less power than single hop techniques.

Multihop techniques can also effectively overcome some of the signal propagation outcomes experienced in long-distance wireless communication [6]. WSN may also have additional application dependent components such as a location finding, system, power generator, and mobilizer (Fig. 1). Sensing units are usually composed of two sub units: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally related with a small storage unit, controls the procedures that make the sensor node collaborate with the other nodes. A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells).

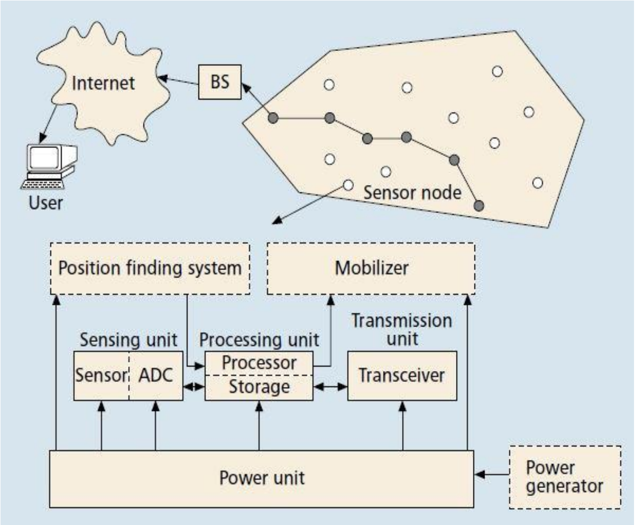

Figure-1:

II. CHARACTERSTICS OF WSN

The important characteristics of a WSN include

- Limited Power consumption for nodes using batteries or energy harvesting
- Ability to run with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes

- Scalability to large scale of exploitation
- capacity to survive hard environmental conditions
- Easy to use
- Unattended operation
- Power consumption

III. WSN & ADHOC NETWORK

As WSNs are lots of similar to traditional wireless ad hoc networks, important differences exist which greatly influence how security is achieved [4]. In [8], I. F. Akyildiz et al proposed the differences between sensor networks and ad hoc networks are:

1. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.

2. Sensor nodes are densely deployed.

3. Sensor nodes are lying face down to failures due to harsh environments and energy constraints.

4. The topology of a sensor network changes very frequently due to failures or mobility.

5. Sensor nodes are limited in computation, memory, and power resources.

6. Sensor nodes may not have global identification.

IV. PROTOCOL STACK

The protocol stack used in sensor nodes. It has physical, data link, network, transport, and application layer. Layer of protocol stack are defined as follows [8]:

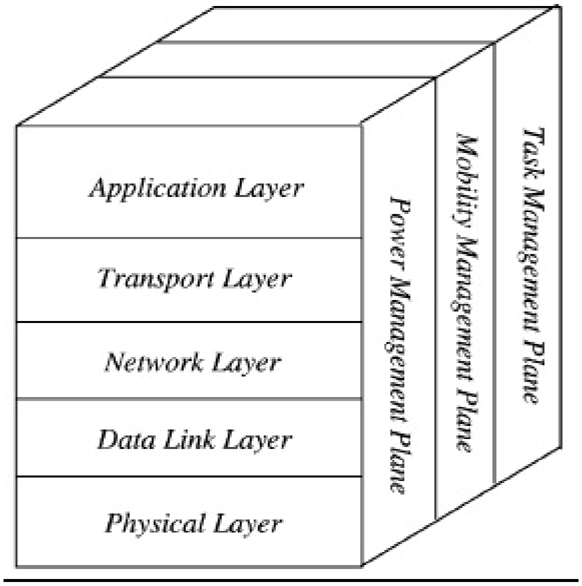

Figure 2: Protocol Stack for WSN [8]

1. Physical layer: It provides a channel for the transmission. This is responsible for frequency selection, data encryption, , signal deflection, carrier frequency generation, and modulation.

2. Data link layer: This is responsible for the multiplexing of signals i.e data streams, data frame detection, medium access, and error control; as well as ensuring reliable node-to-node and point-to-multipoint connections.

3. Network layer: This layer is responsible for providing the assignment of addresses and provides the path to transfer the packets.

4. Transport layer: This is responsible for specifying reliable transmission and how packets are completely transferred to the destination end.

5. Application layer: Its responsibility is specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.

Power management plane: It handles the power which is used by the sensor node. For example, when sensor node not getting any type of messages from one of its neighbor then sensor node should keep turn off the receiver or after receiving the message sensor node should turn off its receiver. the sensor node may turn off its receiver. This is to avoid getting duplicated messages.

Mobility management plane: It is used to concentrate on the location of sensor nodes. It detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes.

Task management plane: It balances and schedules the sensing tasks given to a specific region.[8]

V. CHALLENGES

In wireless sensor network there are several challenges like battery depletion problem, physical means mechanical or electrical problems, environmental degradation. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. Sensor nodes carry limited, normally not changeable, power sources. Therefore, while traditional networks aim to get high QOS (quality of service) of the wireless sensor network provisions, sensor network protocols must primarily concentrate on power conservation [4].As we know that wireless sensor networks use the concept of wireless ad-hoc network so it has self organizing behavior. So in WSN, topology changes dynamically. Sensor network do not have any predefined infrastructure so it does not use any regular topology.

So in wireless sensor networks, several challenges have to be overcome to achieve the potential of WSNs. One of the challenges in the successful use of WSNs comes from the limited energy of the individual sensor nodes. Significant current research has therefore been directed at reducing energy consumption at the sensor nodes. In the hardware front, energy efficient components have been developed, and in the software front, power aware routing, low complexity coding, and low power data processing algorithms have been examined. Although these advances are expected to increase the lifetime of the wireless sensor nodes, due to their extremely limited energy budget and environmental degradation, node failure is expected to be quite common.

The inherent nature of WSNs such as unattended operation, battery powered nodes, and harsh environments are major challenges. One of more challenge is to ensure that the network is connected. The connectivity of the network can easily be interrupted due to unpredictable wireless mediums or channels, early depletion of energy of node, and physical tampering by hostile users.[7]

VI. Cuts In Wireless Sensor Networks

ONE of the unique challenges in mobile ad-hoc 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 multi-hop 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.[1].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 **cuts** in wireless sensor network many problems may arise like a wired network means data loss problem arises, means data reach in a disconnected route.

VII. 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.

VIII. Cut Detection In WSN

We consider the problem of detecting cuts between nodes of a wireless sensor network. We assume that there is a special designated node in the network, which we call the *source station or node*. Suppose source station may be a base station that serves as a mediator 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 got disconnected from the source, we can say that a disconnection from Source station so can say that event has happened for u. When a cut happens in the network that does not separate a node u from the source node, we can say that connected, but a Cut Occurred Somewhere so can say another event has occurred for u. [1]

By "approximate location" of a 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. [1].

IX. Cut Detection Techniques

Kleinberg describes detection of network failure paper [10]. The problem of network partition in sensor networks has been raised in several papers. As noted by Shrivastava *et. al.* [9], the challenges posed by the possibility of network partitioning in WSNs has been recognized in several papers (see, e.g. [10], [11], [12]) but the problem of detecting when such partitioning occurs seems to have received little attention. As we concluded after the study in paper[2], the work done by Shrivastava et. al. is the only one that develop the anomaly of detecting partitions in wireless sensor networks. They developed an scheme for detecting o linear cuts, which is a linear separation of n nodes from the base station.

Kleinberg *et. al.* have studied the problem of detecting network failures in *wired* networks, and proposed schemes for the case when k edges fail independently [13], [14] So finding the location of break in the network has done by Shrivastava et.by developing the algorithm for cut detection in paper [2] .In paper [2] Shrivastava developed a simple, low-overhead technique to find and locate the cuts or partitions or break point of the network in sensor networks. In this paper, they tried to reduce the communication cost for detecting linear cuts by using only a small number of sentinel nodes. Different sets of sentinels however, may lead to communication costs, and an important second-order optimization would take this effect into account. Another way to minimize the communication in the network would be to make the cut detection more decentralized. These are both very practical questions and natural directions for future work. In this paper we have limited ourselves to *linear* cuts. This is an important and natural class of cuts, but a richer set of cuts would include *circular cuts*, *rectangular cuts*, and *polygonal cuts* [10][9].

In paper [7] Myounggyu Won, focused on a more general partition detection problem – which is the *destination-based cut detection* problem. Unlike the traditional cut detection problem, they tried to find partitions of the network between a node which may be sender and any node in a set of given destinations. They first proposed a Point-to-Point Cut Detection protocol (P2P-CD). P2P-CD allows a sender or a source station to track or catch a cut with respect to any destination node. After that they proposed two schemes to address the destination based cut detection problem. This is the point-to-point cut detection protocol (P2P-CD) which enables each node to be able to detect a partition with respect to any destination node. This protocol significantly minimizes the energy consumption when coupled with an underlying routing protocol at the cost of the knowledge on partial global topology. Their second algorithm was the robust and energy efficient cut detection for multiple sinks (RE-CDM) is a more small solution in that it does not need data on global topology, nor node's place information. [7].This algorithm was designed for network scenarios with a small number of sink nodes.

In paper [11], we have concluded two different techniques to detect network partitioning. Both methods are based on the notion of border nodes and their successful identification. With both systems one is able to distinguish node failure from network partition, with both systems primarily differing in terms of flexibility against failure and network load. These mechanisms explicitly select the best suited nodes and are also able to distinguish node failure from network partitioning. Both our approaches have unique advantages. The centralized approach generates a by far lower message overhead compared to the distributed approach.

It is in its structure much simpler, but burdens one single node far more than the rest of the nodes. The centralized approach also has some critical system states. For example during the time between server failure and the time when all active nodes registered at the new server the network is completely unmonitored. The same problem occurs during the time when a new server has to be elected in a separated partition. The server election phase itself could be a complex and costly task in terms of network load and system downtime.

The distributed approach is far more flexible against node failure. Multiple partnerships make sure that a single or more failing nodes only reduce the monitored area of the affected nodes temporarily. That also has the effect that there is no downtime in that system except if a large number of nodes fail or an extremely unfortunate combination of nodes fail simultaneously. That also makes the system more stable against malicious nodes trying to disrupt the system. These positive properties of course come at a cost. The distributed approach loads the network far more than the centralized approach.[11]

X. 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 efficient cut detection scheme has been proposed and implemented so far.

REFERENCES

[1] Cut Detection in Wireless Sensor Networks : Prabir Barooah, Harshavardhan Chenji, Radu Stoleru, and Tamas Kalm´ ar-Nagy

[2] Detecting Cuts in Sensor Networks: Nisheeth Shrivastava Subhash Suri Csaba D. T´oth

[3] A Partition Detection System for Mobile Ad-Hoc Networks: Hartmut Ritter, Rolf Winter, Jochen Schiller

[4] Attacks in Wireless Sensor Networks :Rishav Dubey, Vikram Jain, Rohit Singh Thakur, Siddharth Dutt Choubey

[5] "A Survey on Sensor Setworks," : I. F. Akyildiz et al IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102–112.

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of the ACM Mobi- Com'00, Boston, MA, 2000, pp. 56–67.

[7] A Destination-based Approach for Cut Detection in Wireless Sensor Networks : Myounggyu Won, Student Member, IEEE, and Radu Stoleru, Member, IEEE

[8] Akyildiz, I.F., Su, W., ankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey. Computer Networks Journal (Elsevier), Vol. 38, No.4 (2002)pp. 393-422.

[9] G. Dini, M. Pelagatti, and I. M. Savino, "An algorithm for reconnecting wireless sensor network partitions," in European Conference on Wireless Sensor Networks, 2008, pp. 253–267.

[10] Detecting Cuts in Sensor Networks: Nisheeth Shrivastava Subhash Suri Department of Computer Science, University of California, Santa Barbara, CA 93106, USA. {nisheeth,suri}@cs.ucsb.eduCsaba D. T´oth Department of Mathematics, Room 2-336, MIT,Cambridge, MA 02119, USA.toth@math.mit.eduY.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[11] A Partition Detection System for Mobile Ad- Hoc Networks Hartmut Ritter, Rolf Winter, Jochen Schiller Institute of Computer Science Freie Universität Berlin, Germany {hritter, winter, schiller}@inf.fu-berlin.de

[12] M. Hauspie, J. Carle, and D. Simplot, "Partition detection in mobile ad-hoc networks," in 2nd Mediterranean Workshop on Ad-Hoc Networks, 2003, pp. 25–27.

[13] P. Barooah, "Distributed cut detection in sensor networks," in 47th IEEE Conference on Decision and Control, December 2008, pp. 1097– 1102.

[14] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: A jammed-area mapping service for sensor networks," in IEEE Real Time System Symposium, 2003.