Review Article on Various sensor networks with Inter-Node connectivity Failure Issue

Gagandeep singh*,Amandeep Kaur

*Student of masters of technology Computer Science, Department of Computer Science Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

Assistant Professor, Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

* kakamaan27@gmail.com; anu_virk10@yahoo.com.

Abstract-Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, autonomous, low-power, low-cost, small-size devices using sensors to cooperatively collect information through infrastructureless ad-hoc wireless network. It consist of various nodes which move and collect the information and dissemaninate it through other sources which process this information. Node failure is common problem in wireless sensor network Due to Number of nodes interconnected with each other so volgyed of information in between them.In this paper we illustrate various types of sensor networks and various node failure issues which would be addressed in next article.

Keywords-WSN, WSN TYPES,NODES,ISSUE;

I. INTRODUCTION[1]

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communication digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate in short distance [1].

These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following ways -

• Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.

• Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused. A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-

determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities.

Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

TYPES OF SENSOR NETWORK

- Terrestrial WSN
- Underground WSN
- Underwater WSN
- Multimedia WSN
- Mobile WSN

Terrestrial WSN -Terrestrial WSNs typically consist of hundreds to thousands of inexpensive wireless sensor nodes deployed in a given area, either in an ad hoc or in a pre-planned manner. In ad hoc deployment, sensor nodes can be dropped from a plane and randomly placed into the target area. In pre-planned deployment, there is grid placement, optimal placement 2-d and 3-d placement models.

In a terrestrial WSN, reliable communication in a dense environment is very important. Terrestrial sensor nodes must be able to effectively communicate data back to the base station. While battery power is limited and may not be rechargeable, terrestrial sensor nodes however can be equipped with a secondary power source such as solar cells. In any case, it is important for sensor nodes to conserve energy.

Underground WSN-Underground WSNs consists of a number of sensor nodes buried underground or in a cave or mine used to monitor underground conditions. Additional sink nodes are located above ground to relay information from the sensor nodes to the base station. Energy is an important concern in underground WSNs. A key objective is to conserve energy in order to increase the lifetime of network which can be achieved by implementing efficient communication protocol.

Underwater WSN-Underwater WSNs consist of a number of sensor nodes and vehicles deployed underwater. As opposite to terrestrial WSNs, underwater sensor nodes are more expensive and fewer sensor nodes are deployed.

Autonomous underwater vehicles are used for exploration or gathering data from sensor nodes. Compared to a dense deployment of sensor nodes in a terrestrial WSN, a sparse deployment of sensor nodes is placed underwater.

Typical underwater wireless communications are established through transmission of acoustic waves. A challenge in underwater acoustic communication is the limited bandwidth, long propagation delay, and signal fading issue.Another challenge is sensor node failure due to environmental conditions. Underwater sensor nodes must be able to self-configure and adapt to harsh ocean environment. Underwater sensor nodes are equipped with a limited battery which cannot be replaced or recharged. The issue of energy conservation for underwater WSNs involves developing efficient underwater communication and networking techniques

Multi-media WSN

Multi-media WSNs have been proposed to enable monitoring and tracking of events in the form of multimedia such as video, audio, and imaging. Multi-media WSNs consist of a number of low cost sensor nodes equipped with cameras and microphones. These sensor nodes interconnect with each other over a wireless connection for data retrieval, process, correlation, and compression.Multi-media sensor nodes are deployed in a pre-planned manner into the environment to guarantee coverage. Challenges in multi-media WSN include high bandwidth demand, high energy consumption, quality of service (QoS) provisioning, data processing and compressing techniques, and cross-layer design. Multi-media content such as a video stream requires high bandwidth in order for the content to be delivered. As a result, high data rate leads to high energy consumption. Transmission techniques that support high bandwidth and low energy consumption have to be developed. QoS provisioning is a challenging task in a multi-media WSN due to the variable delay and variable channel capacity. It is important that a certain level of QoS must be achieved for reliable content delivery. In-network processing, filtering, and compression can significantly improve network performance in terms of filtering and extracting redundant information and merging contents.

Mobile WSN

Mobile WSNs consist of a collection of sensor nodes that can move on their own and interact with the physical environment. Mobile nodes have the ability sense, compute, and communicate like static nodes. A key difference is mobile nodes have the ability to reposition and organize itself in the network. A mobile WSN can start off with some initial deployment and nodes can then spread out to gather information. Information gathered by a mobile node can be communicated to another mobile node when they are within range of each other. Another key difference is data distribution. In a static WSN, data can be distributed using fixed routing or flooding while dynamic routing is used in a

mobile WSN. Challenges in mobile WSN include deployment, localization, self-organization, navigation and control, coverage, energy, maintenance, and data process.

Mobile WSN applications include but are not limited to environment monitoring, target tracking, search and rescue, and real-time monitoring of hazardous material. For environmental monitoring in disaster areas, manual deployment might not be possible. With mobile sensor nodes, they can move to areas of events after deployment to provide the required coverage. In military surveillance and tracking, mobile sensor nodes can collaborate and make decisions based on the target. Mobile sensor nodes can achieve a higher degree of coverage and connectivity compared to static sensor nodes. In the presence of obstacles

The major issues that affect the design and performance of a wireless sensor network are as follows:

1) Hardware and Operating System for WSN

2) Wireless Radio Communication Characteristics

3) Deployment

4) Synchronization

5) Data Aggregation and Data Dissemination

6) Programming Models for Sensor Networks

7) Security

Wireless sensor networks are vulnerable to many attacks because of broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Similar to other communication systems, WSNs have the following general security goals:

- **Confidentiality**: protecting secret information from unauthorized entities.
- **Integrity**: ensuring message has not been altered by malicious nodes.
- **Data Origin Authentication**: authenticating the source of message.
- **Entity Authentication**: authenticating the user/node/base-station is indeed the entity, whom it claims to be:
- **Access control** : restricting access to resources to privileged entities.

- **Availability**: ensuring desired service may be available whenever required.

In addition, WSNs have following specific security objects:

- **Forward secrecy**: preventing a node from decrypting any future secret messages after it leaves the network.
- **Backward secrecy**: preventing a joining node from decrypting any previously transmitted secret message.
- **Survivability**: providing a certain level of service in the presence of failures and/or attacks.
- **Freshness**: ensuring that the data is recent and no adversary can replay old messages.
- **Scalability**: supporting a great number of nodes.
- **Efficiency**: storage, processing and communication limitations on sensor nodes must be considered.

Node Failure Definition and types of Node Failure:[5]

Failed nodes may decrease the quality of service (Qos) of the entire WSN. It is important and necessary to study the fault detection methods for nodes in WSNs for the following reasons [5,6]:

(1) Massive low-cost sensor nodes are often deployed in uncontrollable and hostile environments.Therefore, failure in sensor nodes can occur more easily than in other systems;

(2) The applications of WSNs are being widened. WSNs are also deployed in some occasions such as monitoring of nuclear reactor where high security is required. Fault detection for sensor nodes in this specified application is of great importance;

(3) It is troublesome and not practical to manually examine whether the nodes are functioning normally;

(4) Correct information cannot be obtained by the control center because failed nodes would produce erroneous data. Moreover, it may result in collapse of the whole network in serious cases.

(5) Nodes are usually battery-powered and the energy is limited, so it is common for faults to occur due to battery depletion.

WSN node faults are usually due to the following causes: the failure of modules (such as communication and sensing module) due to fabrication process problems, environmental factors, enemy attacks and so on; battery power depletion; being out of the communication range of the entire network.

The node status in WSNs can be divided into two types [7,8]: 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[7,9], 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.

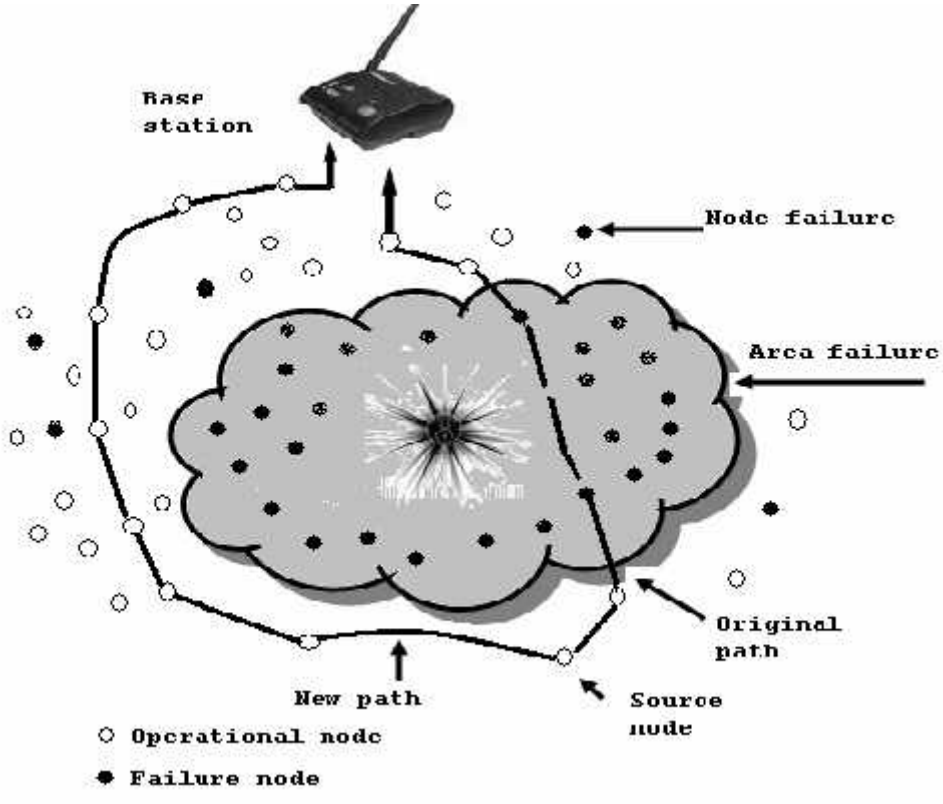

Figure1. Define the classification of node Failure of wireless sensor networks[6]

Types Of Node Failure:

Node Failure can be defined mainly as-

1.Static Node failure

2.Dynamic Node failure.

Static Node failure[5]

Massively parallel systems are often composed of hundreds or thousands of components (such as routers, channels and connectors) that collectively possess failure rates higher than what arise in the ordinary systems. For these systems, new measures have been introduced that can evaluate the capability of a system for gracefully degradation. In the design of such systems, one of the most fundamental considerations is the reliability of their interconnected networks, which can be usually characterized by connectivity of the network topological structure. Resilience of graphs and various types of deterministic networks have attracted significant attention in the research literature. A classical problem in this line of study is to understand failure conditions which the network disconnects and/or starts to offer noticeably lower performance (such as increased routing distance) to its users. In this paper, we investigate the problem of network disconnection by means of simulation in the context of large-scale interconnect networks and understand how static patterns of node failure affect the resilience of such networks.

Dynamic Node Failure

A dynamic discover routing method for communication between sensor nodes and a base station in WSN. This method tolerates failures of arbitrary individual nodes in the network (node failure) or a small part of the network (area failure). Each node in the network does only local routing preservation, needs to record only its neighbor nodes' information, and incurs no extra routing overhead during failure free periods. It dynamically discovers new routes when an intermediate node or a small part of the network in the path from a sensor node to a base station fails. In our planned method, every node decides its path based only on local information, such as its parent node and neighbor nodes' routing information. So, it is possible to form a loop in the routing path. We believe that the loop problem in sensor network routing is not as serious as that in the Internet routing or traditional mobile ad-hoc routing. We are trying to find all possible loops and eliminate the loops as far as possible in WSN.

CONCLUSION AND FUTURE WORK

In this paper, we have presented a dynamic and static node failure for communication between sensor nodes and a base station in a WSN. Paper presents the the basic architecture and types of Wireless sensor networks.

We have reviewed various nodes failure in this paper with a propionate Figure. In Next work we will present the How will detect and avoid these node failures and improve the efficiency of a WSN.

REFERENCES

[1] Akyildiz I.F., W. Su*, Sankarasubramaniam Y., E. Cayirci, " Wireless sensor networks: a survey", *Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology* Atlanta, GA 30332, USA ,Received 12 December 2001; accepted 20 December 2001.

[2] I.F. Akyildiz , et al., "A Survey on Sensor Networks," *IEEE Communications Magazine,* vol. 40, no. 8 ,pp. 102-114, 2002.

[3] Ashish Kumar Srivastava1 and Aditya Goel2 , " Security Solution for WSN Using Mobile Agent Technology " *International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN)* Vol. 1, No. 3, September 2011, ISSN: 2047-0037.

[4] D.Sheela, Srividhya.V.R, Vrushali, Amrithavarshini and Jayashubha J.," A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks", *International Conference on Computational Techniques and Artificial Intelligence (ICCTAI'2012)* Penang, Malaysia. Published:March 2012.

[5] Eric Sabbah, Adnan Majeed, Kyoung-Don Kang, Ke Liu, and Nael Abu-Ghazaleh , "An Application-Driven Perspective on Wireless Sensor Network Security" *Q2SWinet'06, October 2, 2006,* Torremolinos, *Malaga, Spain.* Copyright 2006 ACM 1-59593-486.

[6] Abdulrahman Hijazi, "Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks‖, WOCN", *Second IFIP International Conference, pp. 362-366, June 2005. Zhang Yuyong, Jingde.," Mobile Agent Technology"* , Beijing, Tsinghua University Press, 2003.

[7] Saleh Kassem,Anwar ul jwari,"total system assurance system", *IJCA special issue on wireless information networks and business information system"WINBIS*,2011.

[8] Adrian Perrig, John Stankovic, And David Wagner , "Security In Wireless Sensor Networks" *COMMUNICATIONS OF THE ACM* June 2004/Vol. 47, No. 6 pp53-57.

[9] D.B lange and M.Oshima , "Seven good reasons for mobile agent", *Communication of the ACM* vol.42.no3 pp88-89 2001.

[10] S.Poornima and B.B.Amberker, "Agent Based Secure Data Collection in Heterogeneous Sensor networks", *In proc. of Second International Conference on Machine Learning and Computing IEEE Computer Society* of 2010 pp.116-120.