Fault Tolerance in Real Life Distributed System with Wireless Sensor Network: An Overview

*Md. Mahfuzur Rahman Siam,*Tarikat Ullah,*Farzana Azad *
Department of computer Science and Engineering, State University of Bangladesh, 138, Dhaka 1215

Abstract: *This thesis delves into the critical domain of fault tolerance within real-life distributed systems, with a specific emphasis on wireless sensor networks (WSNs). As WSNs continue to proliferate in applications ranging from environmental monitoring to industrial automation, the susceptibility to faults and disruptions necessitates advanced fault tolerance strategies for ensuring system reliability. The primary objective of this research is to comprehensively explore, analyze, and propose effective fault tolerance mechanisms tailored to the unique characteristics and challenges posed by WSNs in practical scenarios. The investigation begins with an in-depth examination of the various types of faults that can afflict WSNs, including node failures, communication errors, and environmental disturbances. Building upon existing fault models, this research proposes novel.*

Keywords: WSN,Environmental disturbances

1.INTRODUCTION

In the era of interconnected systems and pervasive wireless sensor networks (WSNs), the reliability of distributed systems has become paramount for real-life applications ranging from smart cities to industrial automation. As these systems face an array of challenges, including dynamic network conditions and resource constraints, achieving robust fault tolerance is imperative. This thesis delves into the intricate interplay of fault tolerance within real-life distributed systems integrated with WSNs. Through an exploration of historical failures and real-world scenarios, the research aims to extract valuable insights

as:

encompass understanding the unique characteristics of WSNs, proposing adaptive fault recovery strategies, and evaluating their efficacy through both simulations and practical experiments. The outcomes of this study aspire to advance both theoretical frameworks and practical implementations, offering a roadmap for fortifying the resilience of distributed systems in the face of real-world challenges posed by wireless sensor networks.

2.DIFFERENT TYPE OF FAULT IN RTDS

2.1,Network Fault: A network fault refers to a that inform the development of tailored fault tolerance mechanisms. The objectives

problem or abnormality within a computer network that disrupts its normal operation, leading to degradation or failure of communication between devices or systems. Packet Loss, Packet corruption, destination failure, link failure ect.

2.2. Physical Fault : Physical fault tolerance is a one kind of hardware for tolerance where it cannot examine the front and run time but it only gives the back of for Hardware. Examplesuch as memory, hard disks, CPU and other Hardware devices.

2.3. Software Fault: Software Fault Tolerance involves designing and implementing software systems to detect, mitigate, and recover from faults, ensuring continued and reliable operation in the presence of software-related issues.

2.4. System Fault: System fault tolerance is the capability of a system to continue operating in the presence of faults or failures. It involves redundancy, error detection, and recovery mechanisms to ensure reliability.

2.5. Processor Fault: Processor fault tolerance involves designing systems to withstand and recover from failures in the central processing There are different types of fault which can occur in Real-Time Distributed System. These faults can be classified on several factors such

3. WIRELESS SENSOR NETWORK

A WSN consists of spatially distributed sensors, and one or more sink nodes (also called base stations). Sensors monitor, in realtime, physical conditions, such as temperature, vibration, or motion, and produce sensory data. A sensor node could behave both as data originator and data router. A sink, on the other hand, collects data from sensors. For example, in an event monitoring application, sensors are required to send data to the sink(s) when they detect the occurrence of events of interest. The sink may communicate with the end-user via direct connections, the Internet, satellite, or any type of wireless links.

3.1. BASIC ARCHITECTURE OF WARELESS SENSOR NETWORKS

This a simple service architecture applicable to a sensor network. In this special case, the client wants to acquire information about the surface conditions in the area of interest.

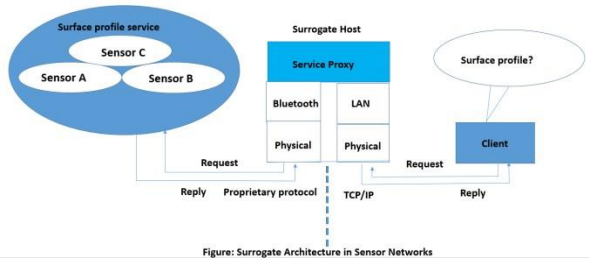


Figure: Surrogate Architecture in Sensor Networks

First, the client requests the surrogate proxy via standardized protocols for the surface profile of a part of the observed area. The unit (CPU), ensuring uninterrupted operation and data integrity in the face of faults.

2.6. Media Fault: Media fault is one kind of fault.Iit's occurs due to Media head crashes.

3.2. SENSOR NETWORK SOFTWARE ARCHITECTURE

The logical view on a sensor network application. The nodes can be contacted only through services of the middleware layers.
They do not perform any individual tasks. The

Distributed Middleware coordinates the cooperation of the services within the network.

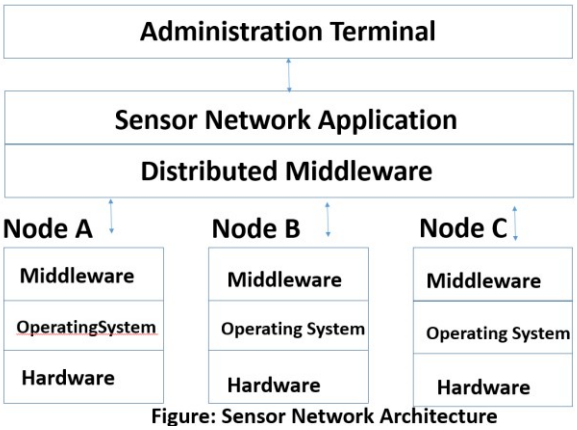


Figure: Sensor Network Architecture

It is logically located in the network layer but it exists physically in the nodes. All layers together in conjuction with their configuration compose the sensor network application. The Administration Terminal is an external entity to configure the network and evaluate the results. proxy communicates with the distributed nodes using a proprietary protocol. The nodes located in the target area try to determine the surface profile using cooperative algorithms and send it to the proxy. The proxy translates the information into standardized protocols and sends them back to the client.

sensor nodes demands reliable communication in dense atmospheres. Ground WSN nodes, often battery-powered and irreplaceable, must efficiently relay information to the Base Station, emphasizing the crucial need for energy conservation strategies.

3.3.2. UNDERGROUND WSNs: Underground Wireless Sensor Networks (WSNs) are placed within the earth's crust for monitoring activities like volcanic conditions. Additional sink nodes above ground transmit information from underground sensor nodes to the Base Station. These WSNs are costlier due to specialized equipment for reliable communication through soil, water, rocks, and challenging interior conditions.

3.3.3. AQUATIC (UNDER WATER)WSNs: Aquatic WSNs involve fewer, costlier sensor nodes and autonomous vehicles dispersed underwater, contrasting with the ground WSNs' dense deployment. Autonomous aquatic vehicles collect data from sparse sensor nodes at sea levels. Communication in aquatic WSNs relies on acoustic wave transmission.

3.3.4. MULTI-MEDIA WSNs: Multimedia Wireless Sensor Networks (WSNs) combine affordable sensor nodes with microphones and It can be connected to the network at any location.

3.3. TYPES OF WSN

According to formerly research paintings completed five forms of WSN are feasible relying upon where in and how sensors are installed up to monitor info. According to these properties of sensor deployment we are able to classify WSNs into five primary sorts namely:

3.3.1. Ground WSNs: Deploying hundreds to thousands of inexpensive Wireless Sensor Nodes (WSN) randomly in a sensing region poses challenges. Random ad hoc diffusion of

affecting the performance, reliability, and
affecting the performance, reliability, and
functionality of a computer network. Here are some common types of network faults:

3.4.1. Packet Loss

Definition: Packet loss occurs when data packets transmitted across a network fail to reach their destination.

Causes: Congestion, network congestion, hardware failures, or errors in network devices.

3.4.2. Packet Corruption

Definition: Packet corruption happens when the data within a packet is altered or damaged during transmission.

Causes: Signal interference, electrical noise, faulty hardware, or software errors. **3.4.3. Destination Failure**

cameras, interconnected wirelessly for data sensing, processing, correlation, and compression. These networks facilitate event monitoring through multimedia applications.

3.3.5. MOBILE WSNs: Mobility WSNs are a no. of transferring sensor with their interplay with sensing atmosphere. Moving sensor nodes have the potential to compute, like nonmoving nodes. Mobility WSNs are utilized in military and other industrial applications.

3.4. TYPES OF NETWORK FAULTS

Network faults can occur in various forms,

Causes: Network congestion, varying packet routes, or fluctuations in network latency.

3.4.7. Latency

Definition: Latency is the delay between the transmission of data and its reception at the destination.

Causes: Physical distance between nodes, network congestion, or processing delays in network devices.

3.4.8. DNS Resolution Issues

Description: DNS resolution issues occur when the Domain Name System fails to translate a domain name into an IP address.

Causes: DNS server outages, misconfigurations, or network connectivity problems can lead to resolution issues.

Definition: Destination failure occurs when the intended recipient of data becomes inaccessible or unresponsive.

Causes: Server outages, software crashes, or misconfigurations leading to the unavailability of the destination node.

3.4.4. **Link Failure**

Definition: Link failure happens when a connection between two network nodes is disrupted or lost.

Causes: Physical damage to cables, hardware failures in network devices, or environmental factors affecting the link.

3.4.5. Congestion

Definition: Network congestion refers to the excessive load on a network, leading to delays, packet loss, and decreased performance.

Causes: High data traffic, inadequate network capacity, or inefficient network design.

3.4.6. Jitter

Definition: Jitter is the variation in the delay of received packets, causing irregularities in the timing of data transmission.

3.5. Fault Detection

Fault detection is the first step in fault management in which faults should be identified by network system. Divides the failure detection approaches into two categories:

3.5.1. Centralized Approach One popular method for locating and identifying the root cause of problems in WSNs is the centralised approach. Typically, a sensor

3.4.9. Routing Errors

Description: Routing errors occur when data is improperly directed through the network, leading to delivery issues.

Causes: Misconfigurations in routing tables, network topology changes, or router malfunctions can result in routing errors.

3.4.10. Firewall Blckages

Description: Firewall blockages happen when network traffic is intentionally blocked by a firewall.

Causes: Security policies, misconfigurations, or malicious activity may lead to firewall blockages.

Addressing these network faults involves a combination of preventive measures, such as robust network design and fault-tolerant architectures, and reactive strategies, including fault detection, troubleshooting, and resolution protocols.

monitor a sensor node's physical component

defect via both hardware and software interface. Since the node only needs to compare the binary outputs of its sensors with pre-defined fault models, self-detection of node failure is quite simple.

3.5.2.2. Neighbor Coordination: Another illustration of fault management distribution is failure detection through neighbor coordination. Before consulting with the node that is logically or geographically centralized is in charge of keeping an eye on and tracking down malfunctioning nodes within the network. By periodically injecting requests into the network, the central node often uses an active detection model to retrieve the statuses of the network performance and individual

sensor nodes. In order to locate and identify the malfunctioning or suspect nodes, it analyzes this data. Furthermore, by comparing the past or present statuses of sensor nodes with the total network information models, the central manager offers a centralized method to avert the possible failure. In conclusion, the centralized technique is effective and precise in identifying certain types of network failures.

3.5.2. Distributed Approach: The distributed approach promotes local decision-making, which disperses fault management throughout the network in an equitable manner. Its objective is to give a node the ability to make certain decisions before interacting with the central node. It is believed the less information needs to be sent to the central node the more decisions a sensor can make. Stated differently, the control center ought not to be notified unless a genuine network malfunction has occurred.

3.5.2.1.NodeSelf-Detection: Several academics have developed a self-detection strategy to

3.7.2.Forward recovery:which resets the network state after a failure.

central node, nodes work together with their neighbors to find and diagnose network issues. Furthermore, a node within a one-hop communication range has the ability to query its neighbors for diagnostic information. This makes it possible for the decentralized diagnostic framework to readily grow, if needed, to much bigger and denser sensor networks.

3.6. Error Diagnosis

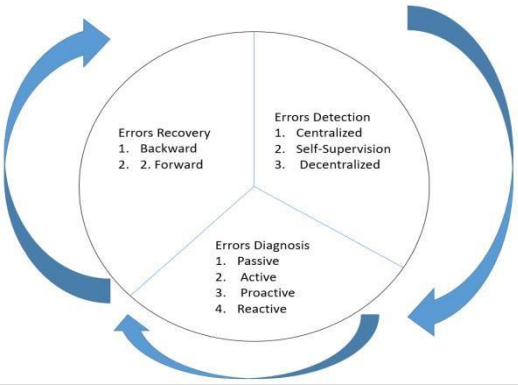
Ensuring fault tolerance in Wireless Sensor Networks (WSNs) is vital. Identifying error types and locating faulty nodes is crucial, often achieved through reference nodes with specific geographical positions. WSN monitoring options include passive (complex, alert-based), active (continuous node messages, lower diagnosis delay, increased traffic), proactive (dynamic data analysis, higher accuracy, increased latency), and reactive (isolating faults through adaptive measures, less complex, more accurate than proactive).

3.7.Fault recovery

Wireless Sensor Networks (WSNs) employ recovery strategies to optimize performance and replace damaged nodes. Two techniques are used:

3.7.1.Backward Recovery: Which records and restores network status using the check pointing technique.

[3] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “Wireless sensor network survey”, (2008) 3469–3475,Elseivier publications.



Backward recovery offers quick and costeffective solutions but faces challenges in storing network status. Forward recovery is

simpler but increases recovery time and network cost with redundancy, making it unsuitable for all sensor nodes.

CONCLUTION

Fault tolerance is crucial in Wireless Sensor Networks (WSNs) to ensure continuous and reliable operations. The diverse strategies, including passive and active monitoring, and proactive and reactive fault recovery, play a pivotal role in maintaining system resilience. Despite challenges like energy conservation and network complexity, ongoing advancements in fault-tolerant techniques underscore the importance of robust fault tolerance in WSNs for their sustained success across various applications.

REFERENCES

[1] Chiara Buratti, Andrea Conti, Davide Dardari, and Roberto Verdone, "An Overview on Wireless Sensor Networks Technology and Evolution " 6869-6896, Sensors 2009.

[4] Daniele Puccinelli and Martin Haenggi, " Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing ", (2005), 19-31, IEEE Circuits And Systems Magazine.

[5] Peng Jiang, "A New Method for Node Fault Detection in Wireless Sensor

[2] Holger Karl and Andreas Willig, "Protocols and Architectures for Wireless

Sensor Networks ", 2005 John Wiley & Sons, Ltd. ISBN: 0-470- 09510-5 ' Networks", Sensors 2009, vol 9, 1282-1294.

[6] M. Yu, H.Mokhtar, M.Merabti, "Fault Management in Wireless Sensor Networks",
IEEE Wireless Communications (2007) 13-19

[7] Sirajul Ameen.C, Mohammed Ashraf.A, Prabakaran.N,"Fault Tolerance Using Cluster in Wireless Sensor Network",IJARCSSE (2014), Volume 4, Issue 4, 351-356.

[8] Chun Lo, Jerome P. Lynch, Mingyan Liu, "Distributed Reference-Free Fault Detection Method for Autonomous Wireless Sensor Network", IEEE Sensors Journal, (2013) 2009- 2019 .

[9] Myeong-Hyeon Lee, Yoon-Hwa Choi, "Fault detection of wireless sensor networks" 31 (2008) 3469–3475,Elseivier publications
[10] Arunanshu Mahapatro , Pabitra Mohan Khilar "Online Distributed Fault Diagnosis in Wireless Sensor Networks" (2013) 71:1931–1960, Springer Science Business Media NewYork 2012.

[11] Bhaskar Krishnamachari, Sitharama Iyengar, "Fault-Tolerant Event Region Detection in Wireless Sensor Networks" 53(2004), IEEE Transactions for computers
[12] Jinran C.