A Survey on Fault Tolerance in Wireless Sensor Networks

Luciana Moreira Sá de Souza
SAP Research
Karlsruhe, Germany
Email: luciana.moreira.sa.de.souza@sap.com

Harald Vogt
SAP Research
Karlsruhe, Germany
Email: harald.vogt@sap.com

Michael Beigl
Technische Universität Braunschweig
Braunschweig, Germany
Email: beigl@ibr.cs.tu-bs.de

***Abstract*— The reliability of wireless sensor networks (WSN) is affected by faults that may occur due to various reasons such as malfunctioning hardware, software glitches, dislocation, or environmental hazards, e.g. fire or flood. A WSN that is not prepared to deal with such situations may suffer a reduction in overall lifetime, or lead to hazardous consequences in critical application contexts. One of the major fault recovery techniques is the exploitation of redundancy, which is often a default condition in WSNs. Another major approach is the involvement of base stations or other resourceful nodes to maintain operations after failures. In this paper we present a survey of approaches to fault tolerance and detection techniques in WSNs in both theoretical and application driven research. We provide a taxonomy of faults and classify the surveyed approaches according to their ability of detecting and recovering from faults.**

I. Introduction

Advances in embedded systems technology have made it possible to build wireless sensor nodes, which are small devices with limited memory, processing power, and energy resources [1]. Due to the low cost associated to these devices, it is possible to conceive the deployment of large-scale wireless sensor networks (WSN) with potentially thousands of nodes [7].

Recently, the usage of WSN to monitor storage regulations of hazardous materials in chemical plants was investigated by the CoBIs project[1]. In this critical industrial environment a high degree of dependability is required. In order to be considered dependable, WSNs must offer characteristics such as: reliability, availability and maintainability.

Availability to a large extend depends on fault tolerance to keep the system working as expected. Availability on the service level means that the service delivered by a WSN (or part of it) is not affected by failures and faults in underlying components such as single nodes or node subsystems. In WSNs, the failure of such components is almost unavoidable. Most detection and recovery techniques therefore aim at reducing *MTTR* (the amount of time required for detecting and recovering from a failure) as much as possible.

We conducted an investigation on frequent faults that occur on real world WSN deployments and the techniques used to detect and overcome these faults. As indicated by deployment reports [27][41][20][43][39], the installation of large-scale sensor networks for real world applications is not a trivial task and can lead to innumerous failures. What works in theory not always performs as expected in practice.

In these WSN deployments, it is common to have a node providing functionality to its neighbors. Multi-hop routing is a simple example of such a service, where nodes forward messages on behalf of each other. Often, nodes assume dedicated roles such as *clusterhead*, which implies the responsibility for certain tasks. For example, a clusterhead could aggregate sensor data before it is forwarded to a base station, thereby saving energy. Nodes with stronger hardware capabilities can perform operations for other nodes that would either have to spend a significant amount of energy or would not be capable of performing these operations.

These services, however, may fail due to various reasons, including radio interference, de-synchronization, battery exhaustion, or dislocation. Such failures are caused by software and hardware faults, environmental conditions, malicious behavior, or bad timing of a legitimate action. In general, the consequence of such an event is that a node becomes unreachable or violates certain conditions that are essential for providing a service, for example by moving to a different location, the node can no further provide sensor data about its former location.

In some cases, a failure caused by a simple software bug can be propagated to become a massive failure of the sensor network. This results in application trials failing completely and is not acceptable in safety critical applications. Hence, our aim is to clarify the requirements for maintaining high level availability in WSNs, and to investigate the tools and mechanisms utilized in WSN research and engineering for fault detection and recovery.

In this paper, we concentrate on enhancements of service availability in WSNs through the use of fault tolerance techniques. We present a survey of approaches to fault detection and recovery techniques in WSNs. We provide a taxonomy of faults and classify the investigated approaches according to their ability to detect and tolerate faults.

This paper provides an overview of the relation of fault tolerance with other areas of research, described in section III, followed by section IV, which presents faults

[1] http://www.cobis-online.de/