Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 104 (2017) 380 – 384

Procedia Computer Science

ICTE 2016, December 2016, Riga, Latvia

Reliability of Sensor Nodes in Wireless Sensor Networks of Cyber Physical Systems

Igor Kabashkin[a,*], Jörg Kundler[b]

[a]*Transport and Telecommunication Institute, 1 Lomonosova iela, Riga, LV-1019, Latvia*
[b]*DFS Deutsche Flugsicherung GmbH, Am DFS Campus 8, Langen D-63225 Germany*

Abstract

Sensors are a crucial component of any intelligent control system. Wireless sensor networks are one of the most rapidly developing information technologies and promise to have a variety of applications in Next Generation Networks, Internet of Things and for mission critical and safety relevant applications. Reliability is one of the most important attribute of such systems. In the paper Markov model for reliability analyses of sensor node in wireless sensor networks is proposed. It is shown that reliability of the sensor node depends on the strategy of it monitoring and is unimodal function of test period. For passive part of sensor node, the optimal time for test of functionality is defined.

Peer-review under responsibility of organizing committee of the scientific committee of the international conference; ICTE 2016

Keywords: Sensor node; Wireless sensor networks; Reliability

1. Introduction

Wireless sensor networks (WSNs) are one of the most rapidly developing information technologies and promise to have a variety of applications in Next Generation Networks (NGNs) and Cyber-physical system (CPS). Wireless Integrated Network Sensors combine sensor technology, signal processing, computation, and wireless networking capability in integrated systems[1]. Cyber-physical system addresses the close interactions and feedback controls between cyber components and physical components, where cyber components refer to the sensing and communication systems, while the physical components comprise of a wide range of systems in practice.

* Corresponding author. Tel.: +371-29215392.
E-mail address: kiv@tsi.lv

Peer-review under responsibility of organizing committee of the scientific committee of the international conference; ICTE 2016
doi:10.1016/j.procs.2017.01.149

CPS is expected to play a major role in the development of next-generation smart energy systems and data centres. Innovative computational methodologies such as green and energy efficient cyber-physical system design have become critical to enable the sustainable development of such systems.

WSNs are spatially distributed systems which consist of dozens, hundreds or even thousands of sensor nodes, interconnected through wireless connection channel and forming the single network. Fig. 1 represents an example of a WSN[2]. Here we can see a WSN which consists of twelve sensor nodes and a network sink, which also functions as a gate. Each sensor node is a device which has a transceiver, a microcontroller, and a sensitive element (see Fig. 2)[2]. Usually sensor node is an autonomous device.

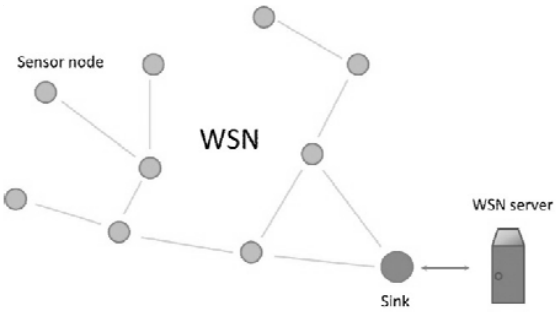

Fig. 1. An example of a WSN[2].

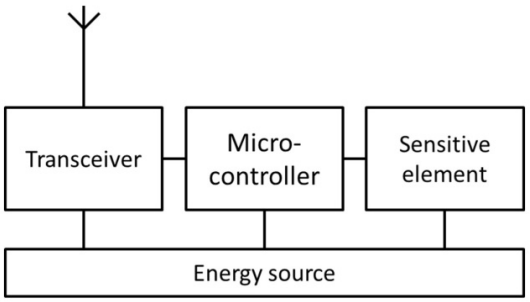

Fig. 2. Sensor node inner structure[2].

Reliability and data integrity is an important attribute of CPS. For some application fields, which have high demands in terms of reliability, it is particularly important to ensure the reliability of the network. At present, most researchers study wireless sensor network reliability from networks topology, reliable protocol and application layer fault correction[3,4].

Sensor node fault types mainly include hardware failure and communication channel fault[5], communication channel fault is generally transient fault that cause by disturbance, obstacle and so on.

The paper examines a focus on the reliability of the sensor node based on periodic test operations, which are conducted to identify the reliability of communication channel.

The rest of this paper is organized as follows. In Section 2 some important works in the area of reliability of WSN sensor nodes are reviewed. In Section 3 the main definitions and assumptions are presented and a model of reliability of sensor nodes in WSN of Cyber Physical Systems is proposed. In Section 4 the conclusions are presented.

2. Related works

The paper[6] presents a survey on existing data transport reliability protocols in wireless sensor networks (WSNs). Authors review several reliability schemes based on retransmission and redundancy techniques using different combinations of packet or event reliability in terms of recovering the lost data using hop-by-hop or end-to-end mechanisms.

The paper[7] presents a survey on existing reliability models in wireless sensor networks.

Most WSNs reliability assessments are based on graph theory and probability theory. Connectivity reliability[8,9,10,11] investigates the probability that the network is still connected for a given period of time under the case of some nodes or links failure. Performance reliability[12,13] analyzes the end-to-end delay, packet delivery rate, and other network parameters.

WSNs reliability is influenced by many factors such as component failure, environmental influences, task changes, and network update. These factors and network behavior are difficult to be described or calculated by mathematical models. Network simulation becomes an important method to analyze network reliability.Monte Carlo[14], Petri nets[15], Bayesian networks[16], and other simulation methods have been used.