Computer Communications 69 (2015) 22–37

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

A survey on fault tolerance in small and large scale wireless sensor networks

Samira Chouikhi [a,b,*], Inès El Korbi [a], Yacine Ghamri-Doudane [c], Leila Azouz Saidane [a]

[a] National School of Computer Science, CRISTAL Lab, University of Manouba, 2010, Tunisia
[b] Université Paris-Est, LIGM Lab, 5 Bd. Descrates, Champs sur Marne 75420, France
[c] L3i Lab, University of La Rochelle, Av. Michel Crépeau, La Rochelle CEDEX 1, 17042, France

ARTICLE INFO

Article history:
Received 3 March 2014
Revised 27 April 2015
Accepted 1 May 2015
Available online 3 June 2015

Keywords:
Fault tolerance
Failure recovery
Wireless sensor networks

ABSTRACT

Fault tolerance is one of the most important wireless sensor networks requirements. It ensures that the network continues to function correctly even when some components fail. In fact, fault tolerance is a need in this type of networks due to sensor node characteristics, radio communications and hostile environments in which these networks are deployed. In this survey, we give an overview of WSN mechanisms that provide or improve the fault tolerance property of wireless sensor networks. However, the different solutions presented in this survey are not only intended to mechanisms dedicated to fault tolerance, but they also include all the mechanisms allowing the prevention of fault occurrence such as energy aware routing and data aggregation and compression. Besides the classification of fault tolerance mechanisms according to the tasks they target (data management, flow management), we also propose a new classification based on the network size, since the performance of the majority mechanisms depends on the size in terms of geographical area and number of nodes. Thus, a well performing protocol conceived for small networks may be inadequate for large networks and vice versa.

1. Introduction

In these recent years, wireless sensor networks (WSNs) [1] have attracted more and more attention. In fact, these networks, composed by a large number of small and cheap sensors, are deployed in several domains (military, industry, agriculture, space, environment, *etc.*). This deployment faces new challenges due to the specific characteristics of sensor (small size, limited battery, limited memory, *etc.*). Many problems are due to the energy depletion and the infeasibility of battery recharge or replacement. The hostile environments in which WSNs are deployed play a great role in the failure of some components, and even of the whole network. All these problems raise the need to provide some mechanisms that mitigate these inadequacies and help the WSN to fulfill its expected functioning, even in fault presence, to improve the fault tolerance.

In the literature, different researches focused on studying fault tolerance at different levels in the WSNs. These techniques cover the whole fault tolerance procedure from fault detection to its recovery. However, to our best knowledge, there are few papers that survey fault tolerance mechanisms and compare their performance in terms of used technique, complexity, and energy at once. Moreover, all these surveys are relatively old, so they do not account for recent works and techniques.

In [2], the authors studied the manner in which the fault tolerance is addressed in different applications. In fact, this work presented five application categories: node placement, topology control, target and event detection, data gathering and aggregation, and sensor monitoring and surveillance. For each application, Liu et al. discussed some representative research works that provide fault tolerance in an application level. de Souza et al. [3] gave an overview on different WSN fault sources: sensor node, communication network, sink node and application. Then, a classification of failures was presented. Moreover, the authors studied some detection techniques that can be used in WSNs. Furthermore, they differentiated between two recovery mechanism categories: active replication and passive replication. However, this classification omitted many fault tolerance techniques that are very interesting and that can improve the reliability of WSNs. In [4], Alwan and Agarwal focused on fault tolerant routing, so they described only one WSN fault tolerance aspect. They classified the solutions in two main classes based on the technique used to improve data transmission. The first technique is the retransmission, in which the source node sends their data over an established path, and if this path fails to forward the information, the source retransmits those

* Corresponding author. Tel.: +216 97680730.
E-mail addresses: samira.chouikhi@univ-paris-est.fr (S. Chouikhi), ines.korbi@ensi.rnu.tn (I. El Korbi), yacine.ghamri@univ-lr.fr (Y. Ghamri-Doudane), leila.saidane@ensi.rnu.tn (L. Azouz Saidane).

http://dx.doi.org/10.1016/j.comcom.2015.05.007
0140-3664/

data through another path. The second technique is the data replication that performs by sending different copies of the same data over multiple paths.

As we said before, there are few works that considered comparison of fault tolerance approaches based on their performance criteria and they do not consider the network size; while, the fault tolerance algorithms proposed for small sized networks differ completely from those proposed for large scale networks. In this paper, we attempt to survey different mechanisms that improve fault tolerance at different WSN levels, and we classify them in two main classes: mechanisms used in small scale WSNs and mechanisms for large scale WSNs. Our classification is influenced by the fact that many mechanisms are dependent on the number of deployed nodes, and by consequence, if they perform well in a small scale network, they may not be adequate in a large scale context.

The rest of this paper is organized as follows: In Section 2, we describe some fundamental WSN fault tolerance concepts and classify the faults according to their type. In Sections 3 and 4, we present the mechanisms that improve fault tolerance in small and large scale WSNs. In Section 5, we study two typical applications of WSNs. We conclude by Section 6 in which we give new challenges that must be studied to provide a robust fault tolerance solution.

2. Fundamental concepts of fault tolerance in WSNs

Before presenting the different fault tolerance mechanisms in WSNs, we introduce some fault tolerance fundamental concepts. For instance, we present the used terminology and the different levels at which faults may occur in the network.

2.1. Terminology

- A **fault** is any inherent weakness (defect) of a system that leads to an error.
- An **error** is an incorrect or undefined system state that may lead to a failure.
- A **failure** is a system deviation from its expected service, which affects its intended functionality.
- The **fault tolerance** is the ability of a functional unit or system to continue to perform a required function in the presence of faults or errors.
- The **fault detection** consists in detecting faulty functionality in a system by self-diagnosis or cooperative diagnosis.
- The **fault recovery** is the recuperation of correct functionality, after the fault detection, by repairing or replacing the failed component. In WSNs, some fault tolerance mechanisms exploit component redundancy or replication to recover from faults.

As any system is conceived to deliver some services, a WSN is deployed to deliver some particular services. In general, a WSN is expected to *collect information* about a zone of interest, *detect an event* or *track a target* over a specific region. Hence, the two major tasks of this type of networks is sensing the expected information correctly and transmitting the sensed data to a sink that collects and processes or sends them to a processing center. According to the application, a disruption that faces one of the two tasks may affect the quality of the delivered service. Thus, any fault or error that prevents a node from sensing and/or transmitting is considered as a failure at a node level. However, this failure may have no impact on the WSN functioning if the application requirements tolerate some failures at the sensed information level and the data are still reaching the sink. In opposite, some critical applications require that each node functions correctly.

2.2. Fault origins in wireless sensor networks

Different works have been proposed to classify the fault origins [2,3]. The two classifications are similar, but the point of view differs. The first classification is from the point of view of WSN components, while the second is a classification from the point of view of the system. According to the classification in [3], faults can occur either due to nodes, network or sink problems as follows.

2.2.1. Node faults

The node failure is caused by either the hardware (sensing unit, CPU, memory, network interface, battery, *etc.*) or the software (routing, MAC, and application) malfunction. Moreover, a hardware failure may lead to a software failure. For instance, if the battery energy falls below a level, the sensing unit may provide incorrect readings that prevent an application of data acquisition from performing properly. However, some services of the node are still provided even with the failure of some hardware components. As an example, a node can be used to route data even if it delivers incorrect readings. In fact, some applications of WSNs tolerate the failure of sensing unit if they did not require a high degree of coverage or some redundant nodes are deployed in the same vicinity. However, the depletion of the limited energy is considered as a critical common failure as it prevents the node from providing any service. Thus, any mechanism that minimizes the energy consumption and prolongs the node lifetime is considered as a preventive fault tolerance solution in WSNs.

2.2.2. Network faults

The WSN applications require the collection of information from sensor nodes and the transmission of the data toward a sink. This task may be disturbed by some faults occurring in some links or some paths (routing). In WSNs, the nature of wireless links makes it prone to faults due to many factors such as the interferences between the nodes of the WSN or between co-existent networks, and the collisions of packets that cause the loss of the transmitted data. As a second source of faults, the paths built by the routing protocols may lead to packet dropping and data loss. Thus, the routing protocol must respect the application requirement during the selection of routes. For instance, an application of periodic data collection tolerates the delay generated by a new path selection, while a critical application of fire detection requires that the alert packet reaches the sink in short delay even in presence of faults. Moreover, the fact that the data are sent to the sink arises the importance that the network is connected.

2.2.3. Sink faults

The sink is an essential component in WSNs, hence its failure leads to the failure of the whole network if no fault tolerance mechanism is implemented to overcome this failure. As for a node, the faults can occur in hardware or software. However, unlike sensor nodes, the sink has no energy constraints.

Owing to the classification presented in [2], faults can be classified into four classes according to the four layers in which the fault is occurred: hardware layer, software layer, network communication layer and application layer.

2.2.4. Hardware layer

In this layer, faults are the malfunction result in one or many sensor components, such as memory, battery, sensing unit and wireless radio. There are three basic reasons that cause failure: the quality of cheap components, the limited energy that may result some incorrect readings when it falls below a certain threshold, and finally, the hostile environment in which the network is deployed that affects many components performance, in particular the communication radio.

2.2.5. Software layer

This layer is represented by two components: the system software, such as operating system, and the middle-ware which includes communication, routing and aggregation. The bugs are the main WSN error source in this layer. One solution is to implement each program in different versions. At the middle-ware level, a large number of protocols are expected to support fault tolerance.