Journal of Network and Computer Applications 45 (2014) 168–180

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Adaptive failure detection in low power lossy wireless sensor networks

Fatima Zohra Benhamida, Yacine Challal*, Mouloud Koudil

Laboratoire de Méthodes de Conception de Systèmes, Ecole nationale Supérieure d'Informatique, Algiers, Algeria

ARTICLE INFO

Article history:
Received 23 November 2013
Received in revised form
18 July 2014
Accepted 21 July 2014
Available online 1 August 2014

Keywords:
Failure detector model
Adaptive timer-based techniques
Lossy links
Low-power WSN

ABSTRACT

In this paper, we investigate the use of failure detectors (FD) in Wireless Sensor Networks (WSN). We provide a classification of FD with respect to some WSN criteria. The focus will be on energy depletion and lossy links. We then propose a new general FD model tailored to WSN constraints, called Adaptive Neighborhood Failure Detector for Low-power lossy WSN (AFDEL). AFDEL provides adaptive local failure detection robust against packet loss (intermittent failures) and saves the use of energy, bandwidth and memory storage. Furthermore, we introduce in AFDEL model an adaptive timer strategy. This strategy offers the possibility to customize the dynamic timer pattern with respect to application requirements in terms of completeness and accuracy. We illustrate the use of this strategy by proposing three failure detection techniques based on AFDEL general model. As a part of this work, we give a stochastic based approach for timer adaptation. We evaluate all techniques using implementation on MiXim/Omnet++ framework. The overall experiments show that AFDEL achieves better trade-off between accuracy/completeness and detection/recovery period compared to static timer approach FaT2D (Benhamida and Challal, 2010) and HeartBeat timer-free technique (Aguilera et al., 1997). Moreover, using adaptive timer strategy in local interaction/detection makes it possible to reduce energy consumption and the overall exchanged data overhead.

1. Introduction

The detection of process crash in distributed systems is a critical problem that designers have to cope with. Thus, failure detectors have been introduced as a fundamental service able to help the development of resilient distributed systems. Its importance has been revealed by Chandra and Toueg (1996) who proposed the abstraction of unreliable failure detectors in order to circumvent the impossibility of consensus in asynchronous environments. Unreliable failure detectors, namely FD, can informally be seen as a per process oracle which periodically provides a list of probable crashed processes. This concept has been implemented for distributed systems with wired connectivity and abundant energy. In this paper, we consider the study of FD in wireless sensor networks, which is a special case of distributed systems with new constraints on resources and radio link quality.

Wireless sensor network (WSN) consists of spatially deployed autonomous sensors, working cooperatively to monitor observed phenomena. It is an enabling technology for several applications such as surveillance of environmental conditions, battlefield tracking, and medical assistance. This kind of networks presents the following properties: (1) a node does not necessarily know all the nodes of the network due to the storage capacity limitations. It can only send messages to its 1-hop neighbors, i.e. those nodes that are within its transmission range; (2) the network is not completely connected because of radio range limitation, which means that a message sent by a node might be routed through a set of intermediate nodes until reaching the destination; (3) links are prone to failures and may momentarily drop messages during transmission; (4) nodes are equipped with very small autonomous batteries. Communication protocols have to consider this limitation for efficient energy consumption; (5) WSNs are prone to a variety of malfunctioning conditions due to the potential deployment under uncontrolled and harsh environment and to the complex architecture and energy depletion.

Fault tolerance is, therefore, one of the critical issues in WSN. This requires a consideration of the ability to cope with node crashes by detecting failed nodes, isolating them and eventually recovering routes to which they belonged. Notice that implementing FD, initially proposed for distributed systems, requires a special design to respond to WSN constraints. Some researchers have proposed few failure detectors tailored to WSN. However, most of them rely on assumptions that are not realistic with respect to WSN constraints and operation environment.

In this paper, we shall survey the main failure detectors proposed for distributed systems and the possibility to apply them to WSN. For this reason, we introduce a set of classification criteria to

* Corresponding author.
E-mail addresses: f_benhamida@esi.dz (F.Z. Benhamida), y_challal@esi.dz (Y. Challal), m_koudil@esi.dz (M. Koudil).

http://dx.doi.org/10.1016/j.jnca.2014.07.028
1084-8045/

compare these different FD. The focus will be on energy depletion and lossy links for the reason that resource limitation and reliable communication represent one of the most relevant constraints for WSN (Guo et al., 2012; Mouradian et al., 2014; Abreu et al., 2014). Furthermore, we study the few proposed FD particularly designed for WSN. As we aim to enhance the failure detection paradigm for WSN, we propose a new FD class $\diamond S^{al}$. This class adapts FD properties for dynamic systems using local interactions for failure notification. The contributions of our work are manifolds:

1. We introduce failure detection model specifically designed for WSN, respecting WSN constraints and limitations: energy, memory, wireless transmission limitations (packet loss, intermittent connectivity), and non-complete graph topology.
2. The message exchange pattern is based on the local exchanged information among neighbors and not on global exchanges among nodes in the system. This allows us to define efficient energy consumption strategy.
3. It tolerates intermittent failures due to lossy links and adapts crash detection procedure using an adaptive timer.
4. It offers the possibility to customize the timer adaptation technique to application requirements in terms of completeness and accuracy.

The paper is organized as follows: in the next section, we recall failure detectors background. Then, in Section 3, we present classification criteria to study FD in the perspective of applying them to WSN. We rely on this classification to present related works. In Section 4, we introduce a new FD model that fits low-power lossy WSN. The general algorithm and its properties are given in Section 5. We explain its timer adaptation strategy. In Section 6, we illustrate the use of this FD model and its dynamic timer by proposing three timer adaptation techniques. In the next section, we present performance evaluation analysis through extensive simulations using Omnet++/MiXim and comparison with respect to existing solutions. We end up this paper with conclusions.

2. Failure detector: definitions

In their seminal paper (Chandra and Toueg, 1996), Chandra and Toueg define unreliable failure detector as a per process oracle which periodically provides a list of probable crashed processes in the system. Authors have proposed eight classes of unreliable failure detectors formally characterized by two properties: completeness and accuracy. Completeness requires that FD eventually suspect every process that actually crashed, while accuracy limits the mistakes that FD can make. The FD is unreliable in the sense that it may not suspect a crashed process or can erroneously suspect a process of having crashed while it is correctly working. The FD can later on remove the process from its list if it believes that it was a mistaken suspicion. The eight possible classes, given in Table 1, are defined from the following completeness properties:

1. *Strong completeness*: Eventually, every process that crashes is permanently suspected by every correct process.
2. *Weak completeness*: Eventually, every process that crashes is permanently suspected by some correct processes.

The two completeness definitions can be combined with the following four accuracy properties:

1. *Perpetual strong accuracy*: No process is suspected before it crashes.
2. *Perpetual weak accuracy*: Some correct processes are never suspected.
3. *Eventual strong accuracy*: There is a time after which no correct process is suspected.
4. *Eventual weak accuracy*: There is a time after which some correct processes are never suspected.

In what follows, we classify some related works and then investigate the use of FD in WSN with respect to WSN constraints.

Table 1
Unreliable failure detector classes.

Completeness	Accuracy			
	Strong	Weak	Eventually strong	Eventually weak
Strong	P	S	$\diamond P$	$\diamond S$
Weak	Q	W	$\diamond Q$	$\diamond W$

3. Related works

In this section, we review failure detectors proposed in the literature and analyze the ability to implement them for low-power lossy WSN. Our aim is to analyze how far each FD is suitable for WSN while considering WSN constraints and limitations. In addition to generic FD that have been designed for distributed systems, we consider FD that have been designed specifically for WSN. Our review will follow classification criteria that we defined after deep analysis of existing solutions with respect to WSN constraints that would influence the design of appropriate FD. Namely, we will consider design decisions regarding detection paradigm, network connectivity, radio link failure, and energy consumption.

3.1. Failure detection paradigm

Many failure detection paradigms have been proposed according to system and network models. Some works implement keep-alive methods based on heartbeats, pings or application data messages. Both Aguilera et al. (1997) and Rost and Balakrishnan (2006) have proposed FD solutions based on heartbeats. Heartbeat is a message periodically sent from monitored node to the failure detector to inform that it is still alive. If the heartbeat does not arrive before timeout expires, the monitored node is then considered as faulty. Besides, Sens et al. have proposed in Sens et al. (2008) and Greve et al. (2011a) detection mechanism using ping. Ping is a request message continually sent from a failure detector to monitored node. Upon reception of this query, the node responds with an acknowledgment ACK. If the node fails to send the expected ACK, it is suspected of having crashed. Moreover, Rost and Balakrishnan (2006) rely on application data exchange to monitor faults. In this case, no additional messages are handled for crash detection. Failure detectors will rather use specific-application information transmitted through the network to make suspicion. Note that we can classify these paradigms into two types, depending on timers: the timer-based failure detectors handle timeouts to make suspicions. It is generally implemented for synchronous and static systems where timer delays are fairly predictable. Heartbeat paradigms often use timers awaiting the monitored node's message as proposed in Ceretta Nunes and Jansch-Porto (2004), and Heinzelman et al. (2000). However, the majority of failure detectors for asynchronous and dynamic systems use timer-free paradigm since the timeout estimation cannot be given from the network model (Aguilera et al., 1997; Mostefaoui et al., 2003; Sens et al., 2008; Greve et al., 2011a,b, 2012).