Chapter 15
Voting Median Base Algorithm for Measurement Approximation of Wireless Sensor Network Performance

Nazar Elfadil
Fahad Bin Sultan University, Saudi Arabia

Yaqoob J. Al-Raisi
The Research Council of the Sultanate of Oman, Sultanate of Oman

ABSTRACT

The success of Wireless Sensor Network application monitoring relies on the accuracy and reliability of its nodes operation. Unfortunately, operation deviations of these nodes appear as regular occurrences not isolated events as in traditional networks. This is due to their special characteristics that reduce network manufacturing and deployment costs and maintain the nodes immunity against internal and external conditions. The goal of this chapter is to propose a real-time, distributed, passive, and low resources usage performance-monitoring algorithm that monitors Wireless Sensor Network functionality and isolates the detected deviated nodes from norm operation. Simulation and empirical experiments showed that the proposed algorithm has a slight processing and storage overhead. It is important to mention that these experiments showed that the proposed algorithm has a high reliability in tracking and isolating network nodes problems.

INTRODUCTION

Sensor networks are considered to be one of the most motivating research areas since it has strong effect on the technological developments. What make them popular are their abilities to fit into a smaller volume with some good features such as the low production costs with a more power. In addition to this, sensors can be implemented in any environment with harsh conditions to transmit data to the base station regularly. It is not worthy that Sound Surveillance System (SOSUS) is the

DOI: 10.4018/978-1-4666-4691-9.ch015

first obvious sensor networks application (Chong & Kumar 2003). This system with assistance of acoustic sensors was used in the Cold War to track Soviet submarines. However, around 1980, Defense Advanced Research Projects Agency (DARPA) created Distributed Sensor Networks (DSN) program. While Wireless Sensor Networks (WSNs) are generally classified into two categories; namely: (1) Infrastructure-base, and (2) ad-hoc wireless networks. Wireless ad-hoc networks can be further classified into several categories based on their applications; namely: (a) Mobile ad-hoc networks, (b) Wireless sensor networks, (c) wireless mesh networks, and (d) hybrid wireless networks (Piyush et al. 2012), (Akyildiz, & Wang 2005), and (Hande & Erosy 2010).

Wireless Sensor Network (WSN) is expected to be a new revolutionary technology in the manner of the internet due to its characteristics that allow them to have disposal, small size, and unattended maintenance-free nodes. These characteristics arise because the WSNs designers and manufacturers target a cheap system at a fixed performance not as in the traditional network to improve the performance and hold the price constant over the time. This strategy helps to reduce the overall network resources usage. On the other hand, these characteristics, along with the usage of wireless communication, the event-driven nature of the operating system, the harsh environment the nodes work in and the limited usage of fault-tolerant/ diagnosis tools, reduce node immunity against internal and external interference, such as software bugs. This reduction increases the probability of deviating network nodes operation from their norm; decreases network overall functionality and degrade network collected data reliability even when the network protocols robustness increases such that it combats against worst-case scenarios. For example, in some practical deployments, such as (Ramanathan et al. 2006), (Tolle etal. 2005), and (Zhao 2004), an analysis of network collected data showed a reduction in their quality and quantity to an amount of 49% and 55%, respectively. Nevertheless, these analyses showed that these reductions might cause in some cases a failure of the WSN monitoring.

These deviations occur because of two types of errors; i.e. systematic and transient (Eiman & Badri 2003). The systematic type arises because of hardware faults; such as calibration, reduction in the operating power level, and change in the operating condition. It affects the operation continuously until the problem is solved. The transient arises due to temporary external/internal conditions, such as random environment effects, software bugs and channel interference. This type deviates the operation until the effect disappears.

These two deviation types affect the quality and the quantity of the collected data in network (Nasir 2002), and (Laura 2007). They directly affect individual sensor node measurements and drift them by a constant value; i.e. biased error; change the difference between sensor measurement and the actual value; i.e. drift error; and remain sensor measurements constant regardless of changes in the actual value; i.e. complete failure error. In addition, they directly affect network packets communication and drop them. The indirect effect happens when the deviations affect network collaboration function and reduce network performance in terms of the collected data reliability and increase the use of the network resources.

Tracking and detecting the above discussed deviations in WSN is not flexible as in traditional network because of the factors that affect the monitoring analysis and degrade its efficiency such as the:

- Limited finite energy and communication resources,
- Unavailability of a dominant protocol or algorithm that is suitable to work in all applications,
- Unavailability of global measurement variables due to the use of distributed control protocols that reduce the consumption of network resources,