
Yasmine Djebaili, Department of Computer Science, LaSTIC Laboratory, University of Batna 2, Batna, Algeria
Azeddine Bilami, Department of Computer Science, LaSTIC Laboratory-University of Batna 2, Batna, Algeria

ABSTRACT

This article describes how fault tolerance is an essential issue for many WSN (Wireless Sensor Network) applications such as wildlife monitoring, battlefield surveillance and health monitoring. It represents a great challenge for researchers regarding to the characteristics of sensor nodes which are prone to failures due essentially to their limited resources. Faults may occur, not only when sensor nodes exhaust their energy, but also when the congestion phenomenon emerges, because of a high traffic in the network and limited storage capacity of the sensor nodes. In order to support fault tolerance in WSNs, the authors propose a new scheme which incorporates a link quality estimation algorithm and a congestion detection mechanism to enable nodes that present high quality links to be chosen for routing in a non-congested area in case of faults. Evaluations through simulations under NS2 show that our proposed protocol tolerates faults with a minimum cost relatively to HEEP protocol and improves network’s performances comparatively to other fault tolerant protocols such as EF-LEACH.

KEYWORDS

INTRODUCTION

Wireless sensor network (WSN) is a set of autonomous tiny nodes that are equipped with embedded computing devices interfacing with sensors/actuators. Sensor nodes use short range wireless transmitters and act cooperatively over a wide geographical (indoor or outdoor) area, to route data hop-by-hop towards a central node called sink or base station. With the emergence of IoT (Internet of Things), WSNs become more and more attractive by their integration in a real world of interconnected objects to monitor physical or environmental events through internet (Li & Shi, 2015). Some typical applications are military monitoring, environmental observation, weather checking, traffic control application, detecting location of pollutants, home automation applications, security issues and healthcare to improve the quality of life (Abdul-Salaam et al., 2016). Due to the deployment of a large number of sensor nodes in uncontrolled or even harsh or hostile environments, it is common for the sensor nodes to become faulty and unreliable (Zhao & Govindan, 2003). Fault is an incorrect state of hardware or program as a consequence in the failure of components (Zhao & Govindan, 2003).

DOI: 10.4018/IJDST.2018010104

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Failures in wireless sensor networks can occur for various reasons. First, sensor nodes are fragile, and they may fail due to depletion of batteries or destruction by an external event. In addition, nodes may capture and communicate incorrect readings because of environmental influence on their sensing components. Second, as in any wireless networks, links are prone to failure (Woo et al., 2003a), causing network partitions and dynamic changes in network topology. Links may fail when permanently or temporarily blocked by an external object or environmental condition. Packets may be corrupted due to the erroneous nature of communication. In addition, when nodes are embedded or carried by mobile objects, nodes can be taken out of the range of communication. Third, congestion may lead to packet loss. Congestion may occur due to a large number of transitions from a power saving state to an active transmission state of nodes in response to an event-of-interest (Tilak et al., 2002).

Furthermore, all of the above fault scenarios are worsened by cluster formation and multi hop communication nature of sensor networks. Cluster formation is one of the most important problems in sensor network applications; it can drastically affect the network’s communication energy dissipation. When sensor nodes are organized into clusters, it often takes several hops to deliver data from a node to the cluster head (CH). The collected data could be aggregated and sent hop by hop until reaching the CH (Elmazi et al., 2015). The CH failure causes disconnections and data loss within cluster. Hence, it is crucial to detect and recover the CH failure to maintain normal operation of cluster and the whole network (Akyildiz et al., 2002). Also, failure of the nodes may cause the disconnection of other nodes if they are organized as chain. For all these reasons, we must prevent the occurrence of failures in WSNs.

To address the above-mentioned challenges, we propose a new protocol for fault management of nodes and CHs, called FT-HEEP (Fault Tolerant Hybrid Energy Efficiency Protocol). The proposed protocol is implemented in three layers (physical Layer, Mac Layer and Network Layer).

The remainder of this article is organized as follows: next section introduces the related works. Section 3 presents the proposed mechanisms for detection and recovery of faults in order to make HEEP a fault tolerant protocol. In section 4, we discuss the simulation environment and the obtained results. Finally, section 5 concludes the paper.

RELATED WORKS

Link Quality Estimation

Link quality estimators in wireless sensor networks can roughly be classified in two categories: hardware-based estimators and software-based estimators (Kirubasri & Maheswari, 2016).

Hardware-based estimators include Link Quality Indicator (LQI), Received Signal Strength Indicator (RSSI) and Signal to Noise Ratio (SNR). These estimators are directly obtained from the hardware radio transceiver (Chipcon cc2420, 2009). Their advantage is obvious since they do not require any computation overhead as they are built-in directly on the hardware. However, as it was observed and reported in previous experimental studies, hardware-based estimators do not provide accurate estimate (Lal et al., 2003; Srinivasan, 2006; Polastre et al., 2005), mainly for the following reasons: First, these metrics are measured based on 8 symbols of a received packet and not the whole packet. Second, these metrics are only measured for successfully received packets. Therefore, when a radio link suffers from excessive packet loss, they could overestimate the transmission performance by overlooking the information of lost packets.

Software-based estimators are able to count or approximate either (i.) the reception rate, or (ii.) the average number of packet transmissions/re-transmissions, required before its successful reception. The Packet Reception Rate (PRR) and the Acquitted Reception Rate (ARR) count the reception rate. The first is performed at the receiver side and the second at the sender side. These link quality estimators are simple, yet they have been widely used in routing protocols. The Required Number of Packet transmissions (RNP) counts the average number of packet transmissions/re-transmissions,
Related Content

Global Health Network Supercourse and Cancer Epidemiology: Free Cancer Epidemiology Resources on the Internet
www.igi-global.com/chapter/global-health-network-supercourse-cancer/45568?camid=4v1a

Designing Security Properties-Centric Communication Protocols using a Component-Based Approach
www.igi-global.com/article/designing-security-properties-centric-communication/63632?camid=4v1a
Service Quality Model Evaluation
www.igi-global.com/chapter/service-quality-model-evaluation/55242?camid=4v1a

Evaluating the Java Native Interface (JNI): Data Types and Strings
www.igi-global.com/article/evaluating-the-java-native-interface-jni/202381?camid=4v1a