Expert Systems with Applications 41 (2014) 3703–3711

Contents lists available at ScienceDirect

Expert Systems with Applications

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

Probabilistic fault detector for Wireless Sensor Network

Bill C.P. Lau [a], Eden W.M. Ma [a], Tommy W.S. Chow [a,b,*]

[a] Centre for Prognostics and System Health Management, City University of Hong Kong, Hong Kong, China
[b] Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China

ARTICLE INFO

Keywords:
Fault detection
Wireless Sensor Network
Naïve Bayes
Maximum Likelihood Estimation

ABSTRACT

This paper proposed a novel centralized hardware fault detection approach for a structured Wireless Sensor Network (WSN) based on Naïve Bayes framework. For most WSNs, power supply is the main constraint of the network because most applications are in severe situation and the sensors are equipped with battery only. In other words, the battery's life is the network's life. To maximize the network's life, the proposed method, Centralized Naïve Bayes Detector (CNBD) analyzes the end-to-end transmission time collected at the sink. Thus all the computation will not be performed in individual sensor node that poses no additional power burden to the battery of each sensor node. We have conducted thorough performance evaluation. The obtained results showed better performance can be obtained under a network size of 100-node WSN simulations at various network traffic conditions and different number of faulty nodes.

1. Introduction

The proliferation in Micro-Electro-Mechanical Systems (MEMS) technology, which makes deploying low-cost, large-scale, and dense small sensor nodes to collect information from harsh environment feasible, has resulted in the emerging of WSNs. A WSN may consists of hundreds or thousands distributed autonomous sensors, which equipped with sensing, computation, and wireless communication devices to monitor or collect information from various environments including battle fields, remote geographical regions, industrial plants, and office buildings (Erdelj, Mitton, & Natalizio, 2013; Geeta, Nalini, & Biradar, 2013; Taneja, Krioukov, Dawson-Haggerty, & Culler, 2013). Nowadays, WSNs has been widely applied in many different applications like railway security (Daliri, Shamshirband, & Besheli, 2011), transportation system (Ray, Goel, & Chandra, 2011), environmental monitoring (Othman & Shazali, 2012), forest fire detection (Aslan, Korpeoglu, & Ulusoy, 2012), and healthcare (Alemdar & Ersoy, 2010).

Sink/sensor pair is a common architecture of WSNs. The sensors are in charge of measuring the environmental status, which may vary with time and space; collaborating with each other; and forwarding the measured data to the sink. The sink is responsible for integrating, analyzing data received from sensors and responding users and applications accordingly (Hsieh, Leu, & Shih, 2010). There are two types of sensor deployment: structured and unstructured. In an unstructured WSN, a dense collection of sensor nodes is deployed in an ad hoc manner into the field. Once deployed, the network is left unattended to perform monitoring and reporting functions. The numerous nodes and ad hoc topology make the network maintenance such as managing connectivity and detecting failures very difficult. In a structured WSN, all or some of the sensor nodes are deployed in a planned manner; hence, fewer nodes are required for the same coverage of the unstructured WSN (Yick, Mukherjee, & Ghosal, 2008). This lowers the network maintenance and management cost in a structure WSN.

The design and resource constraints of a wired network and that of a WSN are quite different. Resource constraints of a WSN include limited amount of energy, short communication range, low bandwidth, and limited processing power and storage in each sensor node. Design constraints are application dependent and are based on the monitored environment (Yick et al., 2008). Due to these constraints, the sensor nodes may fail to perform correct operations. Moreover, the connection between sensor nodes is prone to temporary or permanent failure under severe environments. A successful packet transmission from sensor node to sink is relying on correct propagation among sensor nodes; hence, node failure can severely influence the network performance. A diagnosis mechanism becomes necessary to ensure the operations are correct and the data collected are meaningful to the user (You et al., 2011).

As mentioned before, the network life time depends on the sensors' life. As the sensors are often deployed in an uncontrolled or even harsh environment, they are prone to having faults (Lee & Choi, 2008). Compared to traditional integrated semiconductor chips, sensors and actuators boarded on a MEMS node have higher chance to be faulty (Khan, Daachi, & Djouani, 2012). These

---

* Corresponding author at: Department of Electronic Engineering, City University of Hong Kong, Hong Kong. Tel.: +852 3442 7756.

E-mail address: eetchow@cityu.edu.hk (T.W.S. Chow).

0957-4174/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.eswa.2013.11.034

properties pose significant challenges to maintaining high quality of service of WSNs. Therefore, efficient and effective fault management deems to be essential for maintaining a robust WSNs service. Yu, Mokhtar, and Merabti (2007) discussed three phases of fault management process. Fault management aims to identify the faulty sensor nodes, and to exclude them from the network. Fault detection is a basic fault management task in WSNs.

There is a trade-off between prolonging the network lifetime by conserving the energy of individual nodes and maintaining the high quality of network services by implementing complex fault management schemes in the network (Yu et al., 2007). In order to minimize the resources consumption and to preserve the energy of nodes, our proposed method is designed to detect and analyze faulty sensor node(s) using data collected at the sink rather than implementing a complex faulty management scheme. The presented results show the proposed method is effective and reliable. Also, the proposed Naïve Bayes framework is the first of its kind to be deployed for performing WSN faulty node(s) detection. Because of the structure of Naïve Bayes classifier, the proposed method is computational efficient. A simulation environment using Zigbee protocol has been set up for the verification of the proposed method.

In this paper, a novel approach, CNBD was proposed to identify the possible faulty sensor node using Naïve Bayes framework. A new attribute, the end-to-end transmission time of each packet arrived at the sink is analyzed for determining the network status. CNBD does not involve any additional protocol and extra resource consumption of sensor nodes while it suggests a list of suspicious faulty nodes to the user. The rest of the paper is organized as follows. Section 2 discusses the related work. In Section 3, the procedures of CNBD is discussed. Section 4 discusses the simulation environment, results and the possible future development. Section 5 concludes the paper.

2. Related works

2.1. Mechanism of Wireless Sensor Network

WSN is a network consists of sensor devices, called *nodes*, and controller, called *sink*. The nodes, measure the environmental parameters and forward these measurements to the sink, which has no constraint on power, through wireless communication. Fig. 1 shows a simple WSN topology.

There are different communication protocols for WSNs; and each protocol has its own characteristics for different applications. The popular communication protocols include Zigbee/802.15.4, IEEE 1451, WirelessHART, ZigBee IP, and 6LoWPAN. In this paper, the simulator is built using Zigbee/802.15.4 protocol because Zigbee aims at constructing a WSN with low cost, low power consumption, low complexity, and low data transmission rate.

There are two common congestion scenarios: node-level and link-level. Node-level congestion is caused by a buffer overflow in the node when link-level congestion is caused by too many nodes requesting the same node for data transmission simultaneously. Under Zigbee standard, signal from node to sink will travel through the shortest path in normal situation. If any packet losses due to hardware failures or congestions, the signal path will be changed (Fig. 2). It results in higher energy consumption and longer end-to-end packet transmission time.

2.2. Fault detection in Wireless Sensor Networks

Different from wired networks, fault management for WSNs concerns a given region rather than a given link between two nodes. Yu et al. (2007) stated the fault management schemes vary in form of architecture, protocols, and detection algorithms. Generally, the fault management for WSNs can be divided into three phases: fault detection, fault diagnosis, and recovery. In this paper, only fault detection will be discussed.

The fault detection technology can be generally classified as centralized approaches and distributed approaches. Briefly, the sink in the centralized approach usually has uninterrupted power supply and makes the diagnostic decisions by periodically injecting requests or queries to other nodes and waits for replies. In distributed approaches, the updated network status and individual node performance was assessed according to the status reporting messages from nodes or data comparison with the neighbors advancing from the concept in Sengupta and Dahbura (1992).

The recent works on network data fault detection include the use of Takagi–Sugeno–Kang fuzzy inference system (Khan et al., 2012), statistical based Auto-regression (Volosencu, 2012), and Bayesian network (De Paola, Lo Re, Milazzo, & Ortolani, 2013).

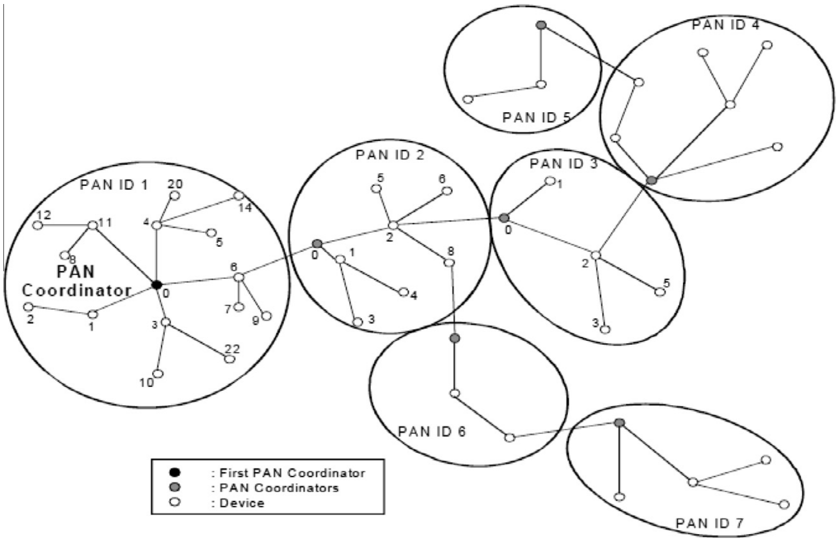

Fig. 1. A simple WSN topology (Fig. 2 in IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – Part 15.4: Wireless MAC and PHY specifications for low-rate WPANs, 2006).