Online Anomaly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring

Osman Salem, Yaning Liu, Ahmed Mehaoua, and Raouf Boutaba, *Fellow, IEEE*

***Abstract*—In this paper, we propose a lightweight approach for online detection of faulty measurements by analyzing the data collected from medical wireless body area networks. The proposed framework performs sequential data analysis using a smart phone as a base station, and takes into account the constrained resources of the smart phone, such as processing power and storage capacity. The main objective is to raise alarms only when patients enter in an emergency situation, and to discard false alarms triggered by faulty measurements or ill-behaved sensors. The proposed approach is based on the Haar wavelet decomposition, nonseasonal Holt–Winters forecasting, and the Hampel filter for spatial analysis, and on for temporal analysis. Our objective is to reduce false alarms resulting from unreliable measurements and to reduce unnecessary healthcare intervention. We apply our proposed approach on real physiological dataset. Our experimental results prove the effectiveness of our approach in achieving good detection accuracy with a low false alarm rate. The simplicity and the processing speed of our proposed framework make it useful and efficient for real time diagnosis.**

***Index Terms*—Anomaly detection, fault detection, Haar wavelet, security, wireless sensor networks (WSNs).**

I. Introduction

In medical applications, implementations of specialized wireless sensor networks (WSNs), known as wireless body area networks, are composed of a set of small sensors with constrained resources, attached or implanted into the body of the monitored patient. These sensors are used to collect various vital signs, while offering freedom to move for patients with long-term diseases [1]. These devices are used to continuously monitor patients at home or in hospitals, and transmit collected data to a portable collection point (e.g., smart phone) with more processing and transmission power.

The collection point is also responsible for raising medical alarms for caregivers, when detecting an anomaly in the physiological data of monitored patients, to quickly react [2]–[4] by taking the appropriate actions. The deployment of WSNs for monitoring will reduce the healthcare costs (overcapacity, sojourn time, number of nurses, etc.), and provide freedom and mobility for monitored patients, by allowing them to fulfill their daily activities while continuously collecting and relaying critical physiological data to healthcare professionals.

Medical sensors with wireless transmission capability are available in the market (MICAz, TelosB, Shimmer, etc.). These sensors are able to collect many vital signs [5], such as heart rate, pulse, oxygen saturation (SpO2), respiration rate, body temperature, electrocardiogram (ECG), electromyogram, and blood pressure (BP).

The noninvasive device called the pulse oximeter is a small clamp sensor mounted on the patient's finger. This device is used to measure the pulse and blood oxygenation ratio (SpO2), through the use of infrared light and photosensor. It exploits the amount of reflected or absorbed infrared light to measure both parameters. The measured information can be exploited to detect asphyxia, insufficient oxygen (hypoxia) or pneumonia. Normal SpO2 ratio is larger than 95%, and when this ratio is lower than 90%, an emergency alarm must be triggered due to respiratory complications.

Sensor readings may be unreliable and inaccurate [6], due to the small size of sensors and their underlying constrained resources (power, computation, and transmission capabilities), which make them susceptible to various errors. For example, an improperly attached device or an additional environmental light (fluorescent lighting) may affect the functioning of pulse oximeter, and cause faulty measurements.

Abnormal values may result from many reasons in WSNs [3], [7], such as hardware faults, corrupted sensors, energy depletion, calibration, electromagnetic interference, signal fading, disrupted connectivity, patient with sweating, detached sensor, malfunction, heart attack, health state degradation, compromised sensors, maliciously injected data for wrong diagnosis, and false treatment, etc. This leads to faulty diagnosis results, a large false alarm ratio, and unreliable monitoring system.

Therefore, it is of paramount importance to detect abnormal measurements (outliers) that deviate from other observations, and to distinguish between sensor faults and emergency situations to reduce false alarms. Abnormal measurements must be excluded to reduce false alarms and unnecessary intervention of healthcare professionals.

With continuous monitoring, the amount of collected physiological data from monitored patients becomes large and intractable. Real-time processing using lightweight algorithms is required to detect abnormal values and to distinguish between patient's health degradation and faulty measurements.

Manuscript received December 1, 2013; revised February 14, 2014; accepted March 8, 2014. Date of publication March 17, 2014; date of current version September 2, 2014.

O. Salem and A. Mehaoua are with LIPADE Laboratory, University of Paris Descartes, 75270 Paris, France (e-mail: osman.salem@parisdescartes.fr; ahmed.mehaoua@parisdescartes.fr).

Y. Liu is with JCP-Connect, 35510 Cession Sevigné, France (e-mail: yaning.liu@jcp-connect.com).

R. Boutaba is with the David R. Cheriton School of Computer Science, University of Waterloo, N2L 3G1 Ontario, Canada (e-mail: rboutaba@cs.uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JBHI.2014.2312214

Therefore, an online anomaly detection mechanism is crucial for reliable operation of medical WSNs, where the detection and isolation of data from faulty or misbehaving sensors can be used to increase the accuracy of medical diagnosis results.

Various anomaly-based detection techniques for sensor fault identification and isolation have been proposed and applied [8]–[11]. Distributed detection techniques identify anomalous values at individual sensors to prevent the transmission of erroneous values and reduce energy consumption. These techniques require resources that are not available in sensors, and their accuracy is lower than centralized approaches, where the central device has a global view for spatio-temporal analysis.

Physiological parameters are usually correlated in time and space. The correlation among these parameters can be exploited to identify and isolate faulty measurements, in order to ensure reliable operations and accurate diagnosis results. This is based on the fact that there is no spatial or temporal correlation among monitored attributes for faulty values.

In this paper, we propose a lightweight fault detection and isolation approach to reduce false alarms, by removing the underlying outliers from faulty sensor measurements. We consider a general deployment scenario, where many sensors are attached to the patient, and are used to monitor different physiological attributes. The collected data are transmitted to a portable device (smart phone) for processing and online analysis. This central device has a global view for spatial and temporal analysis.

The proposed approach is based on the Haar wavelet, nonseasonal Holt–Winters (NSHW), the Hampel filter, and boxplot, and is intended to work on smart phones. It provides online anomaly detection with reduced complexity and memory consumption. The novelty of the proposed approach is a spatio-temporal model used to distinguish faulty measurements from clinical deterioration. The Haar wavelet, Holt–Winters, and Hampel filter are used for spatial analysis, and the boxplot is activated for temporal analysis in order to pinpoint deviated attributes.

The combination of lightweight and robust statistical methods allows discarding false alarms triggered by uncorrelated attributes. The proposed model accurately detects deviations without requiring predefined threshold or labeled training data. Our experimental results on real medical datasets show that the proposed approach is accurate in detecting anomalies, and is reliable in terms of reduced false alarm rate even with the presence of inconsistent data in monitored attributes.

The rest of this paper is organized as follows. Section II surveys related work. Section III summarizes the related techniques and presents our proposed approach for anomaly detection. Section IV presents our experimental results. Finally, Section V concludes the paper.

II. Related Work

Various architectures for vital sign monitoring have been proposed, such as CodeBlue [12], LifeGuard [13], AlarmNet [14], MEDiSN [4], etc. Recent surveys of medical applications using WSNs are available in [1], [15].

However, collected data by WSNs usually have low quality and poor reliability [6], [7], [16]. They are affected by interference, errors, incorrect readings, environmental noise, missing values, inconsistent readings, damaged sensors, etc. Different approaches for anomaly detection have been proposed and applied in WSNs to detect abnormal deviations. Existing solutions in the literature stem from different disciplines such as statistical methods, information theory, machine learning, and data mining.

Statistical methods can be classified into two categories: parametric and nonparametric methods. Parametric methods assume a known underlying distribution of collected measurements. The parameters of the distribution function are calculated in training phase, and are used in test phase to determine if the observation has been emitted by the associated distribution function, i.e., data follow distribution $f(\theta_1)$ before the change and another distribution $f(\theta_2)$ after the change point. Nonparametric methods do not assume a specific distribution for values, and use the distance between data points to measure the deviation between them. Many statistical algorithms have been proposed and tested, such as CUmulative SUM (CUSUM [17]), generalized likelihood ratio ([18]), Holt–Winters (HW [19]), adaptive threshold [20], exponentially weighted moving average, autoregressive integrated moving average (ARIMA), etc.

Information theory focuses on determining the relevance of a certain dataset using measurements such as the entropy [21], e.g., if all observations belong to the same class, the entropy is equal to zero, but once the observations are scattered in different classes, the entropy approaches to one. It is based on the assumption that anomalies induce irregularities in the information content of the analyzed data.

Several machine learning (ML [22]) algorithms have been applied for anomaly detection in WSNs, such as Naïve Bayes, Bayesian network, decision tree (C4.5), neural networks, and support vector machine (SVM). The SVM classifier has gained popularity due to its optimum solution and its simple numerical comparison for data classification.

Several SVM based approaches have been proposed [23]–[25] for anomaly detection in WSNs. Moreover, many nonlinear versions (kernel based) of SVM have been investigated to find a boundary (or hyperplane) that encompasses the majority of normal data in training phase. When the decision boundary is established, any new data outside the boundary is classified as abnormal.

ML algorithms need a preclassified (or labeled) training dataset, which is often skewed or unavailable in real world. Skewed (unbalanced) labeled data occurs when one class is over-represented (e.g., 99% of data are normal) and anomalies are almost not available in training dataset. Constructing a labeled training set is often a laborious and expensive task. To resolve these problems of training data in machine learning methods, data mining (or unsupervised) techniques group similar data in one cluster, and flag the small-size clusters as abnormal. The widely used clustering algorithms [22] are k-means, expectation maximization, hierarchical clustering, fuzzy C-means, and Gaussian mixture models (GMM) [26]. However, unsupervised methods assume normal data lie

in higher density area, and anomalies are relatively rare and have lower density in the neighborhood when compared to the size of normal data cluster. We refer to [27] for comprehensive classification of various detection techniques, and to [22] for more details about various classification and clustering techniques.

One of the most widely used clustering method is k-means [28]. Zhang *et al.* in [29] propose a novel outlier detection and countermeasure scheme based on k-means, K-nearest neighbors (K-NN), static threshold, and transmission frequency. However, K-NN is unsuitable for WSNs, since it requires high computational complexity and large amounts of memory to store training data, in contrast to classification methods which build a model and discard training data after the model creation. Xie *et al.* in [30] propose a new KNN-based anomaly detection method based on hyper-grid that has lower computational complexity than K-NN in WSNs. Siripanadorn *et al.* in [31] use an unsupervised approach for anomaly detection in WSNs, which is based on discrete wavelet transform (DWT) and self-organizing map (SOM). The DWT is used to reduce the size of input data for SOM clustering.

Zhang *et al.* in [7] proposed a survey of different techniques for outliers detection in WSNs, and present a comparative guideline to select the suitable technique based on the characteristics of the used dataset. Liu *et al.* in [9] propose a distance based method to identify insider malicious sensors, while assuming neighbor nodes monitoring the same attributes. Each sensor monitors its one hop neighbors and uses Mahalanobis distance (MD) between measured and received multivariate instances to detect anomaly. However, it is impractical in medical applications to exploit promiscuous mode and to put redundant sensors for monitoring the same parameters.

Yim and Choi in [32] propose a voting based system to detect events. Miao *et al.* in [8] propose a failure detection approach for WSNs, which exploits metric correlations to detect abnormal sensors and to uncover failed nodes. A simple prediction and fault detection method for WSNs was proposed in [33]. The proposed algorithm is based on the detection of deviation between reference and the measured time series by using a predefined threshold, and has been evaluated on three types of faults: short time, long time, and constant fault.

Sharma *et al.* in [34] explore four classes of methods for fault detection: rule-based, estimation-based, time series analysis, and learning based methods. They investigate fixed and dynamic threshold, linear least squares estimation, ARIMA, hidden Markov model, etc. They focus on detecting three fault categories: short, noise, and constant. The authors found no best class of detection methods suitable for every type of anomaly. Rule-based methods require calibrating and tuning threshold parameter, learning methods require training phase, estimation methods cannot classify faults, and time series analysis has the highest rate of false positives.

Chen and Juang in [10] propose a score parameter for anomaly detection in collected data by sensors. This parameter is based on the Hampel filter and kernel density estimator. Zhang *et al.* in [6] note that only limited researchers use spatial and temporal correlation for outlier detection. The temporal dependence means that the current attribute measurement depends on readings at the previous time instants, while the spatial dependence means that the observations from different attributes are correlated.

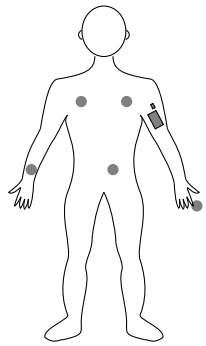

Fig. 1. WSN for remote monitoring of vital signs.

In our previous paper [35], we analyzed real medical dataset and we identified the major cause of high false alarms is due to faulty measurements. In health monitoring, the physiological parameters are heavily correlated. To increase the anomaly detection accuracy, our proposed approach exploits the spatial and temporal dependences among the monitored physiological parameters, to distinguish between faulty measurements and medical emergencies. The objective is to ensure reliable operations of sensors and accurate medical diagnosis results. Sensor measurements tend to be correlated in time and space, and errors are usually uncorrelated from other attributes.

In this paper, we propose a simple and lightweight approach for online anomaly detection in collected data by medical wireless sensors. The proposed framework for reliable vital sign collection is based on the DWT, NSHW forecasting, and the Hampel filter for spatial analysis, and on boxplot for temporal analysis. The objective is to reduce false alarms resulted from faulty measurements, in order to enhance the reliability and the accuracy of the monitoring system.

III. Proposed Approach

We consider a medical deployment scenario for continuous monitoring where N sensors $(S_1, \ldots, S_N)$ are attached or weared by the patient (as shown in Fig. 1). These sensors are used to gather vital signs, and then transmit collected data to a portable device for processing. Each sensor monitors one or many attributes, e.g., pulse oximeter monitors the pulse and SpO2. We denote the collected measurements at the given time instant t by $X_t = (x_{t,1}, x_{t,2}, \ldots, x_{t,p})$, where p is the total number of monitored attributes ($p \geq N$). X_t is a line in the data matrix X given in (1).

$$X = \begin{matrix} X_1 \\ X_2 \\ \vdots \\ X_t \end{matrix} \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,p} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ x_{t,1} & x_{t,2} & \cdots & x_{t,p} \end{bmatrix}. \quad (1)$$

The base station (e.g., smart phone) has more processing power and storage resources than sensors. Therefore, the real-time

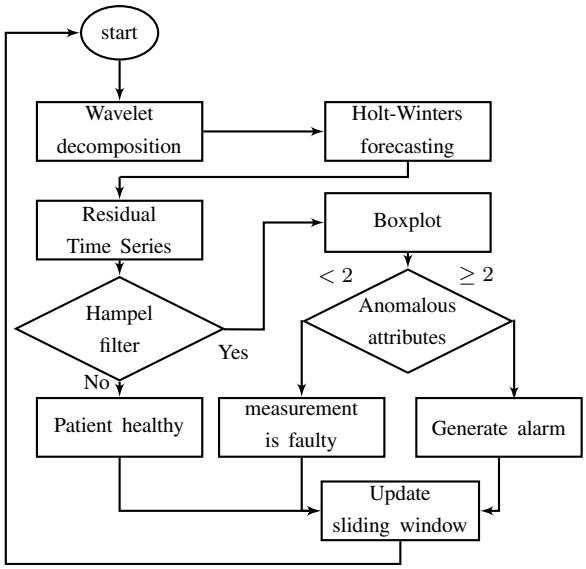

Fig. 2. Flow diagram of the implementation.

analysis of the gathered data on the smart phone is required for early detection of clinical deterioration, and to alert healthcare professionals if any abnormal deviation in the physiological data pattern is detected. The collected measurements are probably of low quality and reliability, due to constrained resources of sensors, environmental conditions, and the deployment context (sweat, detached, damaged sensors, interrupted communications, etc.). The accuracy of this monitoring system relies on the data, where faulty measurements trigger false alarms for the caregiver. Therefore, to increase the accuracy of diagnosis result, faulty values must be detected and isolated in order to reduce the false alarms and prevent faulty diagnosis. The most challenging issue is how to make the difference between sick patient and faulty sensor measurements.

Our proposed approach is based on four algorithms: DWT, NSHW, the Hampel filter, and boxplot. The DWT, NSHW, and the Hampel filter are used to detect spatial deviations, and the boxplot is used for temporal analysis in order to pinpoint suspicious underlying attributes, which are responsible for the detected deviation. The objective is to reduce false alarms, that is to say, to raise alarms only when patient health degrades (respiratory failure, cardiac arrest, etc.).

The architecture of the proposed sequential approach is shown in Fig. 2, where the four algorithms (DWT, NSHW, Hampel, and boxplot) are used to guarantee that alarms will be raised only when the patient enters in critical phase. The DWT is used to decompose the signal into two subsignals: the average of the original signal and the remaining detail after subtracting the average from the original signal. The Haar wavelet is simple, reversible, fast, and memory efficient without requiring a temporary array.

To accurately identify spatial deviations between the values of monitored attributes, we search to identify the deviations in time series associated with the percentage of energy corresponding to the detail signal (E_i). To achieve this task, the NSHW is used to predict the current value ($\hat{E}_i$) and the residual time

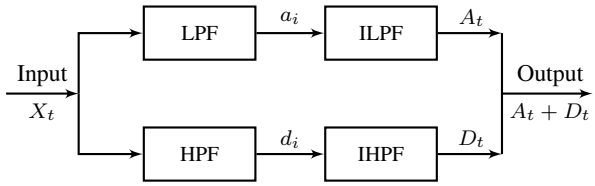

Fig. 3. Filters used in the Haar transform.

series resulted from the difference between the forecasted and measured values ($R_i = \hat{E}_i - E_i$). In contrast to E_i, the values of R_i follow a normal distribution $N(\mu, \sigma)$, where z-score ($\mu - k \times \sigma \leq R_i \leq \mu + k \times \sigma$) can be used to detect outliers.

However, to prevent the distortion of the mean and the variance by outliers, we use the Hampel filter for robust estimation of the μ and σ. When an outlier is detected in R_i, we activate the boxplot to pinpoint the deviated attributes. The choice of boxplot method is due to its small memory requirement, good accuracy with light complexity for examining dataset. As the physiological parameters are heavily correlated, we raise alarms when at least k attributes change in the same time instant. In the next subsections, we develop the algorithm used in each block.

A. Discrete Wavelet Transform

The discrete Haar wavelet transform is used to divide the observations in the vector X_t into two parts: approximation A_t and detail D_t signals. Approximation signal (A_t) is the filtering result of input signal passing through low pass filter (LPF) and inverse low pass filter, and detail signal (D_t) is the filtering result through high pass filter (HPF) and inverse high pass filter as shown in Fig. 3.

Observations in X_t can be reconstructed as the results of inversion filters. We use the Haar wavelet as it is the simplest form of discrete wavelet transform (the smallest computational cost), with only two coefficients $\{l_0 = l_1 = 1/\sqrt{2}\}$ for LPF, and $\{h_0 = -h_1 = 1/\sqrt{2}\}$ for HPF [36]. The signal can be expressed using the matrix L & H with dimension $p/2 \times p$:

$$L = \begin{pmatrix} l_0 & l_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & l_0 & l_1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & l_0 & l_1 \end{pmatrix}.$$

The matrix H has the same structure by replacing the scale coefficients l_0 and l_1 by h_0 and h_1, respectively. The approximation and detail coefficients are obtained as

$$a_i = L \times X_t^T = \frac{x_{t,2i-1} + x_{t,2i}}{\sqrt{2}} \qquad i \in [1, p/2] \qquad (2)$$

$$d_i = H \times X_t^T = \frac{x_{t,2i-1} - x_{t,2i}}{\sqrt{2}} \qquad i \in [1, p/2]. \qquad (3)$$

The approximation A_t (average) and detail D_t (fluctuation) signals are calculated as follows:

$$A_t = a^t \times L = \sum_{i=1}^{p/2} l_{it} \times a_i \qquad t \in [1, p] \qquad (4)$$

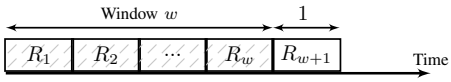

Fig. 4. Sliding window used to estimate statistical parameters.

$$D_t = d^t \times H = \sum_{i=1}^{p/2} h_{it} \times d_i \qquad t \in [1, p]. \tag{5}$$

To detect abnormal deviations between monitored attributes, we monitor the energy of fluctuation signal (D_t) with respect to the total energy of both signals which has been used in [37]:

$$E_i = \frac{\sum_{t=1}^{p} (D_t)^2}{\sum_{t=1}^{p} (A_t)^2 + \sum_{t=1}^{p} (D_t)^2}. \tag{6}$$

The energy ratio signal (E_i) will increase when one or more attributes change. To detect deviations in energy time series ($E = \{E_1, \ldots, E_n\}$), we use NSHWs forecasting to predict the current value of $\hat{E}_i$ as given in (7):

$$\hat{E}_i = L_{i-1} + T_{i-1} \tag{7}$$

where L_{i-1} and T_{i-1} represent the level (baseline) and the linear trend, respectively, and they are calculated as follows:

$$L_{i-1} = \alpha E_{i-1} + (1 - \alpha)\,(L_{i-2} + T_{i-2}) \tag{8}$$

$$T_{i-1} = (1 - \beta)\,T_{i-2} + \beta\,(L_{i-1} + L_{i-2})\,. \tag{9}$$

With initial values of $L_1 = E_1$, $L_2 = E_2$ and $T_2 = E_2 - E_1$. The smoothing constants α and $\beta \in]0, 1[$, and we select $\alpha = \beta = 0.2$ to give more weight for past values, which makes the long-term estimation less sensitive to noise and temporal fluctuations.

The residual time series resulted from the difference between the current value of E_i and the forecasted value $\hat{E}_i$ ($R_i = \hat{E}_i - E_i$) is normally distributed. Statistical based parameters, such as mean (μ) and standard deviation (σ) have been widely used as dynamic thresholds to detect deviations (z-score or $\mu \pm k\sigma$) in normally distributed values. At a confidence level of 95%, the associated value of k is 1.96, and 99% of observations fall within $k = 2.57$ from μ, and 99.73% of observations fall within 3 from μ.

To detect deviations in the residual time series ($R = \{R_1, \ldots, R_n\}$), we use a sliding window of last w observations of R (as shown in Fig. 4) to estimate the statistical parameters (μ and σ) to use in the z-score rule. However, the data in sliding window may contain outliers, which distort and skew the means and the variance toward them, and affect the detection performance. Contaminated data have two underlying effects: masking and swamping problems. Masking occurs when outliers are masked and are not detected, and swamping occurs when normal observation is detected as abnormal (inversion). To avoid these problems, we use robust Hampel filter instead of z-score to detect deviations in residual time series (R).

B. Hampel Filter

The Hampel filter is a sliding window implementation of the Hampel identifier. It was proposed and used as robust alternative to outlier sensitive z-score. To provide robust method for estimating μ and σ in contaminated data, Hampel proposes the use of median and median absolute deviation (MAD) as outlier resistant parameters. We use a sliding window containing the past w values of residual time series $R_i^w = \{R_{i-w}, \ldots, R_i\}$, and we compute the median and the scale (MAD) of R_i^w as follows:

$$\phi_w = \text{median}(R_i^w) \tag{10}$$

$$Std_w = 1.4826 \times \text{median}\{|R_i^w - \phi_w|\}. \tag{11}$$

After replacing the mean μ by the median ϕ_w, and the standard deviation σ by Std_w, the z-score is used to test if the value of R_{i+1} is abnormal:

$$|R_{i+1} - \phi_w| \geq k \times Std_w \tag{12}$$

where k is a threshold value ($k = 1.96$ in our experiments). However, the data in sliding window have zero or near zero MAD under normal condition [10], and we use $Std_w = \max(Std_w, c_1)$ to eliminate false alarms, where c_1 is a predefined constant greater than zero.

As physiological parameters are heavily correlated, and faulty measurements are spatially unrelated with other attributes, the change point detection in the residual time series R can only detect spatial deviations, without any information of the underlying attributes responsible of the occurred change. To identify the abnormal attributes, we activate the univariate boxplot only after the detection of spatial anomaly. The boxplot is used to check temporal deviation in each attribute with low computational complexity. If the number of underlying attributes is smaller than r ($r = 2$ in Fig. 2), we consider the measurement of this attribute is faulty and we discard the data. Otherwise, we raise an alarm for the caregiver to quickly react to the patient health degradation.

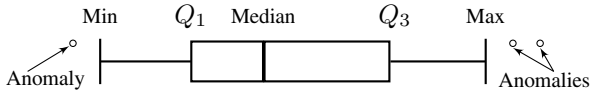

Fig. 5. Boxplot.

C. Box-and-Whisker Plot

The Box-and-Whisker plot or boxplot is a simple and robust outlier detection method. Let $X_i^w = \{x_{t-w,i}, \ldots, x_{t,i}\}$ represents a temporal sliding window of the last w values for the ith monitored attribute. The lower quartile (Q_1 is the 25th percentile) and the upper quartile (Q_3 is the 75th percentile) of X_i^w are used to obtain robust measurements for the mean $\hat{\mu} = (Q_1 + Q_3)/2$, and the standard deviation is replaced by the interquartile range $\hat{\sigma} = IQR = Q_3 - Q_1$. A measurement is considered as abnormal (see Fig. 5) if the following condition is satisfied:

$$x_{t,i} \leq Q_1 - 1.5.(Q_3 - Q_1) \;\vee\; x_{t,i} \geq Q_3 + 1.5.(Q_3 - Q_1). \tag{13}$$

The boxplot method is activated only when spatial deviation is detected. The points outside the whiskers are outliers. Boxplot handles data with low complexity and little memory space, and

Algorithm 1 Anomaly Detection Approach

Apply Haar DWT to get A_t & D_t
Calculate the current value of E_{i+1}
Predict the current value of $\hat{E}_{i+1}$
Calculate the residual $R_{i+1} = \hat{E}_{i+1} - E_{i+1}$
Calculate ϕ_w & Std_w for the last w values (R_i^w)
if $|R_{i+1} - median(R_i^w)| \geq k \times Std_w$ **then**
  for $i = 1$ to p **do**
    $LB_i \leftarrow Q_{1,i} - 1.5 \times IQR_i$
    $UB_i \leftarrow Q_{1,i} + 1.5 \times IQR_i$
    if $((x_{t,i} \leq LB_i)$ || $(x_{t,i} \geq UB_i))$ **then**
      $Alarm$++
    end if
  end for
  if $Alarm \geq r$ **then**
    Raise an alarm for caregivers
  end if
end if

it does not require parameters tuning. The aim of its conditional activation is to pinpoint deviated attributes which provokes energy deviation.

The univariate boxplot is applied on every attribute, and an alarm variable is proposed to count the number of deviated attributes. This variable is incremented while any deviation is detected. When the value of this variable is greater or equal to r, we raise an alarm. For clarification, when the heart rate and respiration rate increase, and the SpO2 decreases, a medical intervention is required. Otherwise, the measurements are considered faulty and no alarm will be raised.

We use a value of $r \geq 2$ in our experiments, as the probability that many sensors are faulty in the same time instant is low. We also consider that the physical check for sensors is necessary when more than r sensors report abnormal values. The proposed method is presented in algorithm 1.

IV. Experimental Results

In this section, we conduct experiments of the proposed approach for anomaly detection in real medical datasets. We further compare and evaluate the performance of our proposed approach with robust MD.

A. Evaluation Setup

To evaluate our proposed model, we use patients' medical records from the multiparameter intelligent monitoring in intensive care (MIMIC) database of Physionet [38]. We use records 221 and 442 containing eight parameters (Blood Pressure, C.O., Heart rate, Pulmonary Artery Pressure, Pulse, RESP, SpO2, Body temperature). We apply our approach on these traces before and after injecting synthetic anomalies at different instants, in order to evaluate the detection accuracy of our proposed approach. We use a sliding window of width $w = 10$ to reduce memory requirement, and we set $k = 1.96$ and $r = 2$.

We begin by showing the variations of physiological attributes in the used datasets. The variations of the heart rate are shown in Fig. 6. The heart rate is measured in beats per minute (bpm), and the normal values for heart rate are inside the interval $[60 - 100]$ for a healthy adult at rest. We can visually identify three zones

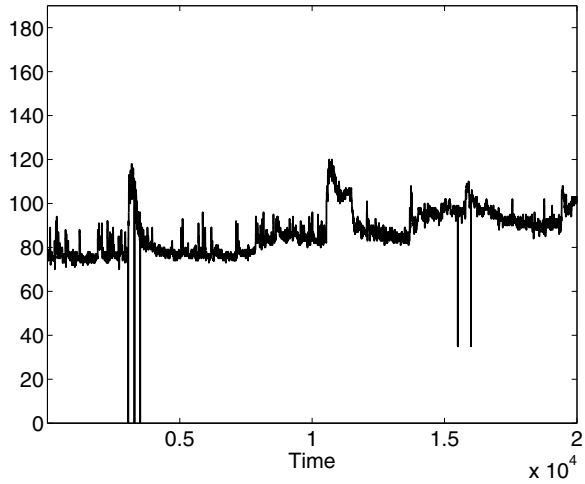

Fig. 6. Heart rate.

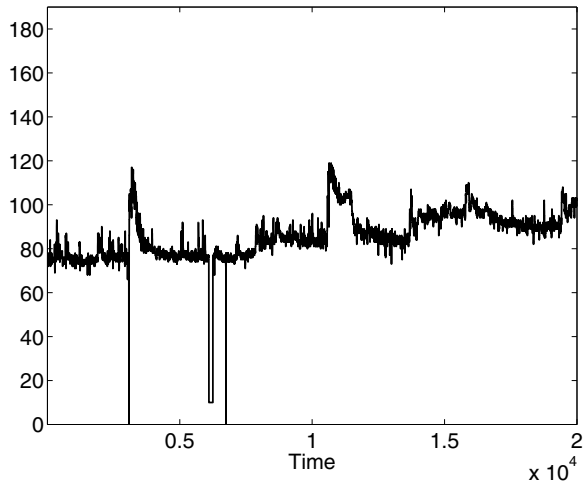

Fig. 7 Pulse.

with anomalies (two zones with five spikes and one zone with abnormal increase of values) in the variations presented in Fig. 6, where we can clearly distinguish that three spikes falling down to zero and two other spikes with values lower than 45 bpm.

The variations of the pulse are shown in Fig. 7. The pulse exhibits four anomalies at different time instants in the heart rate. Usually, the heart rate and the pulse must have the same values and must show the same variations, as they represent the same attribute monitored through two different devices. The heart rate and the pulse are measured in bpm. However, they do not superpose on anomalies when drawing them in the same figure, and different deviations on different time instants appear clearly when comparing Figs. 6 and 7.

Fig. 8 shows the variations of the blood pressure (BPmean) for the monitored patient. The BP is measured in millimeters of mercury (mmHg). Fig. 9 shows the variations of the SpO2 and the respiration rate. The SpO2 must be within the range $[95\% - 100\%]$. A lower value is synonymous of asphyxia, lack of oxygen and heart disease. In Fig. 9, we can notice 3three abnormal readings with zero values for SpO2 followed by normal values. The respiration rate (shown in Fig. 9) is measured

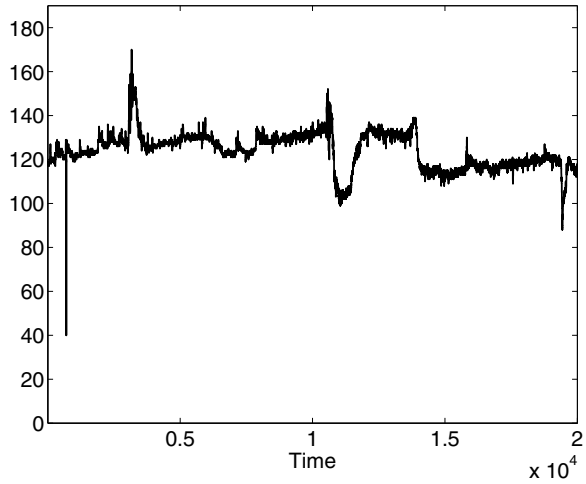

Fig. 8 Blood pressure.

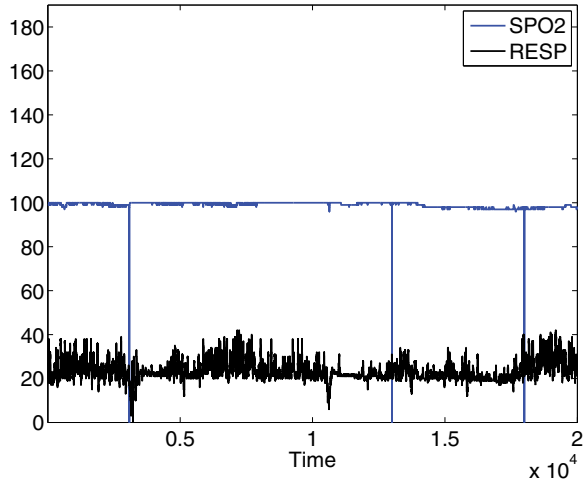

Fig. 9. Respiration & SpO2.

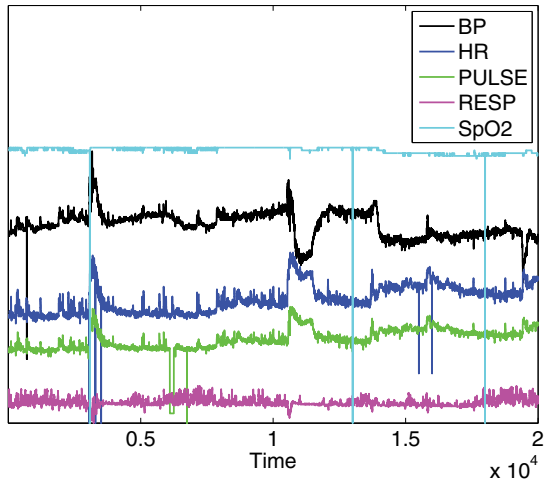

Fig. 10 Variations of five parameters.

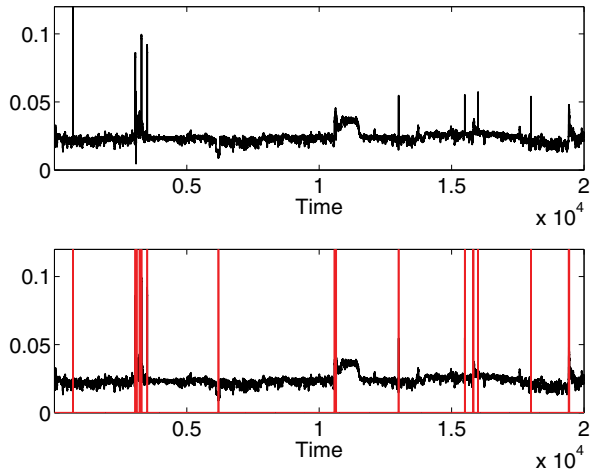

Fig. 11 Energy ratio & raised alarms.

as the number of respiration per minute (r/min), and contains some abnormal values (falling near zero) before the time instant 5000.

As physiological parameters are not the same for all people and depend on many parameters (sex, age, weight, activity, etc.), the use of static interval for anomaly detection heavily depends on many additional dynamic parameters (environmental, ages, activities: rest, moving, awake, sleep, etc.), and these parameters are not easy to set dynamically for anomaly detection.

To prove the correlation between monitored attributes, we show the variations of the five parameters in Fig. 10, where we can notice that clinical emergency induces changes in many parameters at the same time instant. However, there is no spatial correlation among monitored attributes for faulty measurements. It is important to note that some curves in Fig. 10 are shifted for clarifying the shape of their variations. We can visually distinguish three zones of clinical change: the first is around 3500, the second is near to 10 500, and the third around 19 500.

Fig. 11 shows the variations of energy ratio [given in (6)] resulted from DWT. The energy ratio is used to detect spatial deviations, through the application of Hampel filter on the residual time series associated with the difference between forecasted and calculated values of E_t. The raised alarms by Hampel filter for spatial analysis are shown in the bottom of Fig. 11, where we get a high number of false alarms. The prior application of data filtering techniques on each attribute may reduce the noise level by discarding anomalies and retaining good data, but it may also change the shape of variations, and discard interesting events.

We activate boxplot analysis only on the instant with raised alarm by the Hampel filter to achieve temporal analysis on each attribute. Only four alarms are raised after the application of boxplot (with $r = 2$) as shown in Fig. 12. It is important to note the difference between the number of raised alarms by the Hampel filter (see Fig. 11) and those transmitted to caregivers by our proposed approach (see Fig. 12), where we can notice that alarms associated with benign deviation or faulty measurements in one sensor are discarded to reduce false alarms. For example, the raised alarms on the instants 15 500 and 16 000 are false alarms, and they are triggered by abnormal measurements in the heart rate. The same applies for the last two spikes in SpO2.

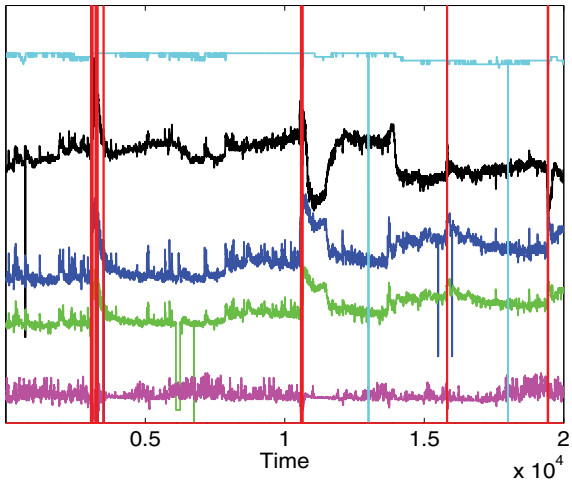

Fig. 12. Raised alarms.

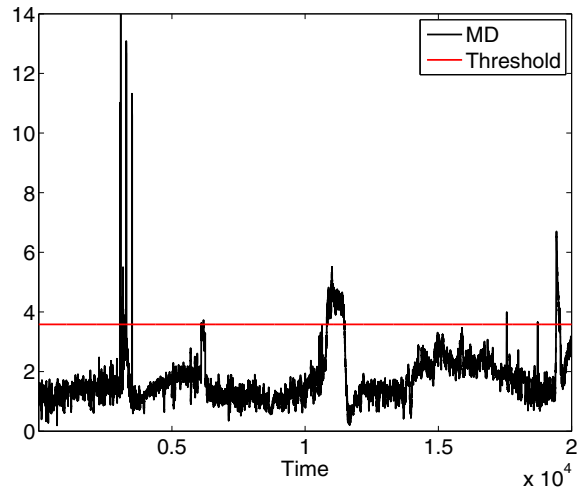

Fig. 13. Robust MD and threshold.

In fact, when the change occurs in many sensors, a medical alarm is triggered by our proposed approach. Otherwise, the measurement is considered to be faulty and will be discarded without raising any alarm. A visual inspection in the variation of monitored attributes in Fig. 10 confirms the accuracy and the utility of raised alarms. However, increasing the value of correlated parameters (r) reduces false alarms, as well as increasing the miss detection rate. The value of r is a tradeoff between detection accuracy and false alarms.

B. Comparison With Robust MD

We compare our proposed scheme with the one proposed in [9], where the MD is used to detect anomaly in gathered data by wireless sensors. We use two different records from the MIMIC database. The reason of using this approach in our comparison is that MD also calculates the distance between measurements by taking into account the correlation between monitored attributes:

$$\mathrm{MD}_t = \sqrt{(X_t - \mu)^T \Sigma^{-1} (X_t - \mu)} \tag{14}$$

where μ is the mean vector ($1 \times p$) and Σ is the covariance matrix ($p \times p$) of these p attributes calculated by a robust estimation method (Orthogonalized Gnanadesikan–Kettenring—OGK) which removes outliers during the estimation of covariance matrix Σ by looking for a subset of training data without anomalies. Many robust estimation methods for covariance matrix of multivariate data have been proposed and used to remove outliers, e.g., minimum volume ellipsoid [39], minimum covariance matrix (MCD [40]), Fast-MCD [40], and deterministic MCD [41].

However, these robust estimation methods and the MD require additional complexity (the inversion of Σ) when comparing to the Haar Wavelet and Boxplot. Furthermore, the robust estimations for $\hat{\mu}$ and $\hat{\Sigma}$ require resources not available on the mobile collection device, nor in the sensor.

MD_t^2 follows chi-square distribution $\chi^2_{p,0.975}$ with p degrees of freedom and 97.5% quantile is used as the static threshold for anomaly detection by MD_t^2 (0.025 significance level for cut-off value). An alarm is triggered when the value of MD_t^2 is greater than the threshold ($\chi^2_{p,0.975}$). The results of applying robust MD over the physiological data are shown in Fig. 13 with the threshold $\sqrt{\chi^2_{5,0.975}} = 3.5822$ (horizontal line). When comparing Figs. 12 and 13, we notice that both methods have good detection accuracy. However, our proposed approach raises only one false alarm and robust MD triggers three false alarms.

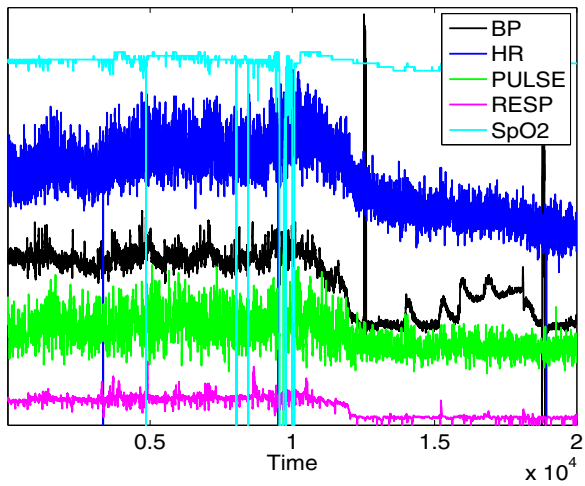

Fig. 14 Parameters for patient 2.

We also use another patient record from MIMIC database (record 442) in our comparison, where Fig. 14 shows the variations of the physiological parameters for this patient. Figs. 15 and 16 show the raised alarms by our proposed approach and by robust MD, respectively. Our proposed approach outperforms the robust MD for both medical data records (associated with patient1 and patient2).

C. Performance Analysis

To conduct performance analysis of the proposed approach, we inject synthetic anomalies at different time instants on different attributes, and we use the receiver operating characteristic

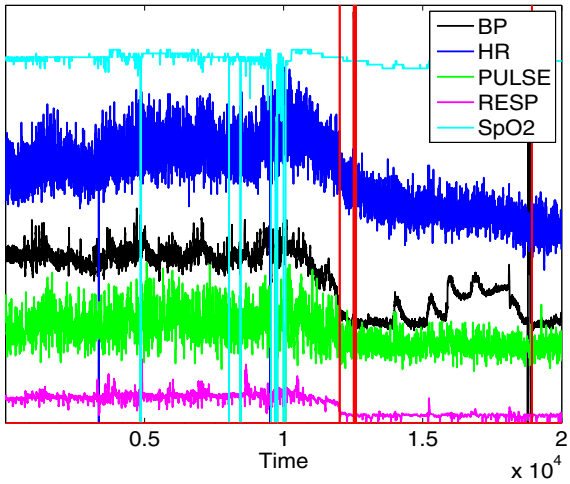

Fig. 15. Raised alarms.

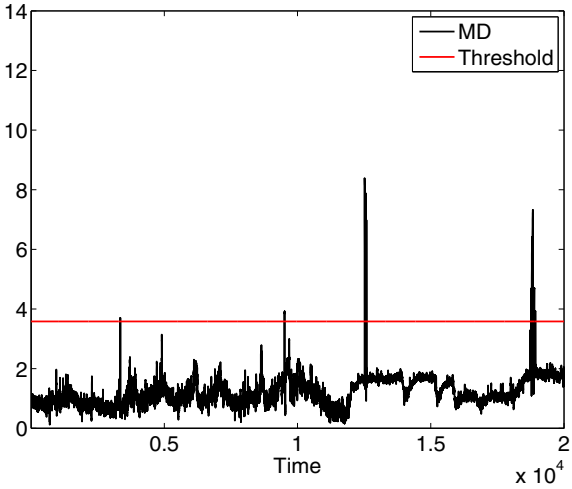

Fig. 16 Robust MD and threshold.

(ROC) curve to show the impact of the threshold (k) on the true positive rate and the false negative rate. The ROC curve presented in Fig. 17 shows the relationship between the detection rate (15) and the false alarm rate (16) for our proposed approach and for robust MD.

$$\text{Detection Rate} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{15}$$

where TP is the number of true Positives, and FP is the number of false positives. The false positive rate is defined as

$$\text{False Positive Rate} = \frac{\text{FP}}{\text{FP} + \text{TN}}. \tag{16}$$

A good detection mechanism should achieve a high detection ratio with a low false alarm rate. Fig. 17 shows that our proposed framework can achieve a DR $= 100\%$ with a FAR $= 7\%$. The performance of robust MD [9] was analyzed over the same medical data records and the result is presented in Fig. 17, where MD achieves a DR $= 100\%$ with a FAR $= 16\%$. The performance of our proposed approach outperforms the robust MD and provides better result.

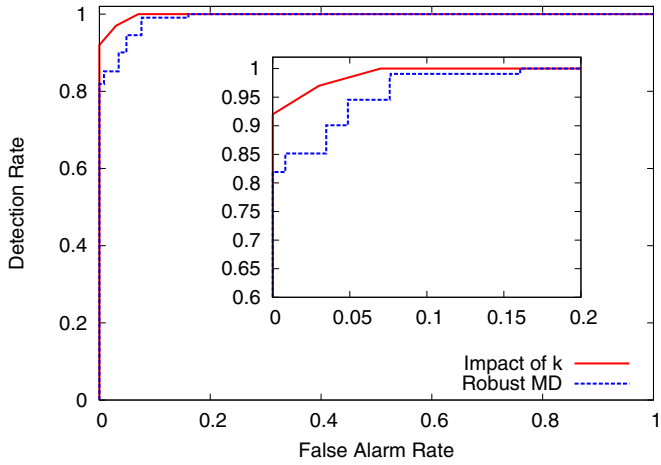

Fig. 17 ROC.

Reducing the false alarm rate will decrease the detection accuracy, and threat to patient safety due to missing alarms. The early detection dramatically reduces the death rate, but false alarms in medical application have a very high cost of needless anxiety. Since no existing approach can achieve 100% of detection rate with 0% false alarm, a tradeoff between low false alarm rate and high detection accuracy is required.

For breast cancer detection, one in four women gets at least one false alarm from a mammogram (FAR=25%). For patients in cardiac unit, a FAR of 20% for an ECG monitor is reported [42]. Schmid *et al.* in [43] report 92% of FAR in pediatric intensive care unit. Therefore, FAR triggered by physiological changes is better for patients' safety than missing detection associated with the monitoring sensitivity which may cause patient harm or death (better-safe-than-sorry logic). The tradeoff achieved by our proposed system is convenient in real-life scenarios according to [43], where one false alarm is triggered in 5.5 h and one check is required. A patient with less than one check in 5.5 h is considered to be under monitored.

V. Conclusion

In this paper, we proposed a lightweight anomaly detection approach for medical WSNs, where faulty measurements and injected malicious data could threat the life of the monitored patient. The proposed approach is based on wavelet decomposition, nonseasonal Holt–Winters, the Hampel filter, and boxplot. It allows achieving spatial and temporal analysis, without prior knowledge of fault signatures. It is suitable for online detection and isolation for faulty or maliciously injected measurements with low computational complexity and storage requirement.

We have tested our proposed approach on real physiological dataset. The experimental results prove that it can improve the efficiency and reliability, by identifying faulty measurements and reducing the number of false alarms. As a future work, we intend to apply this technique for online anomaly detection using the Shimmer platinum development kit [44]. We also plan to implement distributed detection on real sensors to reduce energy wastage due to the transmission of faulty measurements.

REFERENCES

[1] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2688–2710, 2010.

[2] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[3] O. Chipara, C. Lu, T. C. Bailey, and G.-C. Roman, "Reliable clinical monitoring using wireless sensor networks: Experiences in a step-down hospital unit," in *Proc. 8th ACM Conf. Embedded Netw. Sens. Syst.*, 2010, pp. 155–168.

[4] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, T. Gao, W. Destler, L. Selavo, and R. P. Dutton, "MEDiSN: Medical emergency detection in sensor networks," *ACM Trans. Embedded. Comput. Syst.*, vol. 10, no. 1, pp. 1–29, 2010.

[5] T. Yilmaz, R. Foster, and Y. Hao, "Detecting vital signs with wearable wireless sensors," *Sensors*, vol. 10, no. 12, pp. 10837–10862, 2010.

[6] Y. Zhang, N. A. S. Hamm, N. Meratnia, A. Stein, M. van de Voort, and P. J. M. Havinga, "Statistics-based outlier detection for wireless sensor networks," *Int. J. Geograph. Inf. Sci.*, vol. 26, no. 8, pp. 1373–1392, 2012.

[7] Y. Zhang, N. Meratnia, and P. J. M. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE Commun. Surv. Tutor.*, vol. 12, no. 2, pp. 159–170, Apr.–Jun. 2010.

[8] X. Miao, K. Liu, Y. He, Y. Liu, and D. Papadias, "Agnostic diagnosis: Discovering silent failures in wireless sensor networks," in *Proc. IEEE Conf. Comput. Commun.*, 2011, pp. 1548–1556.

[9] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *Proc. IEEE Conf. Comput. Commun.*, 2007, pp. 1937–1945.

[10] Y.-C. Chen and J.-C. Juang, "Outlier-detection-based indoor localization system for wireless sensor networks," *Int. J. Navigat. Observat.*, vol. 2012, no. 1–11, (11 pp.), 2012. Available: http://www.hindawi.com/journals/ijno/2012/961785/cta/.

[11] R. Jurdak, X. R. Wang, O. Obst, and P. Valencia, "Wireless sensor network anomalies: Diagnosis and detection strategies," in *Intelligence-Based Systems Engineering*, A. Tolk and L. C. Jain, Eds. New York, NY, USA: Springer-Verlag, 2011, ch. 12, pp. 309–325.

[12] D. Malan, T. Fulford-jones, M. Welsh, and S. Moulton, "CodeBlue: An ad hoc sensor network infrastructure for emergency medical care," in *Proc. Int. Workshop Wearable Implant. Body Sens. Netw.*, 2004.

[13] K. Montgomery, C. Mundt, G. Thonier, A. Thonier, U. Udoh, V. Barker, R. Ricks, L. Giovangrandi, P. Davies, Y. Cagle, J. Swain, J. Hines, and G. Kovacs, "Lifeguard—A personal physiological monitor for extreme environments," in *Proc. IEEE 26th Annu. Int. Conf. Eng. Med. Biol. Soc.*, 2004, pp. 2192–2195.

[14] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Univ. Virginia, Charlottesville, VA, USA, Tech. Rep. CS-2006-13, 2006.

[15] K. Grgic, D. žagar, and V. Križanovic, "Medical applications of wireless sensor networks—current status and future directions," *Medicinski Glasnik*, vol. 9, no. 1, pp. 23–31, 2012.

[16] X. Ying-xin, C. Xiang-guang, and Z. Jun, "Data fault detection for wireless sensor networks using multi-scale PCA method," in *Proc. Int. Conf. Artif. Intell., Manag. Sci. Electron. Commerce*, 2011, pp. 7035–7038.

[17] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*. Englewood Cliffs, NJ, USA: Prentice-Hall Inc., 1993.

[18] Y. Xie, J. Huang, and R. Willett, "Change-point detection for high-dimensional time series with missing data," *J. Sel. Top. Signal Process.*, vol. 7, no. 1, pp. 12–27, 2013.

[19] J. D. Brutlag, "Aberrant behavior detection in time series for network monitoring," in *Proc. 14th USENIX Conf. Syst. Administrat.*, 2000, pp. 139–146.

[20] S. Bu, R. Wang, and H. Zhou, "Anomaly network traffic detection based on auto-adapted parameters method," in *Proc. 4th Int. Conf. Wireless Commun., Network. Mobile Comput.*, 2008, pp. 601–607.

[21] G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in *Proc. 8th ACM SIGCOMM Conf. Internet Meas.*, 2008, pp. 151–156.

[22] C. M. Bishop, *Pattern Recognition and Machine Learning (Information Science and Statistics)*. New York, NY, USA: Springer-Verlag, 2006.

[23] S. Xu, C. Hu, L. Wang, and G. Zhang, "Support vector machines based on k nearest neighbor algorithm for outlier detection in WSNs," in *Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, 2012, pp. 1–4.

[24] Y. Zhang, N. Meratnia, and P. Havinga, "Adaptive and online one-class support vector machine-based outlier detection techniques for wireless sensor networks," in *Proc. Int. Conf. Adv. Inf. Network. Appl. Workshop*, 2009, pp. 990–995.

[25] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, "Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 518–533, Sep. 2010.

[26] S. Theodoridis, A. Pikrakis, K. Koutroumbas, and D. Cavouras, *Introduction to Pattern Recognition: A MATLAB Approach*. New York, NY, USA: Academic, 2010.

[27] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 3, pp. 1–15, Jul.–Sep. 2013.

[28] P. A. Forero, A. Cano, and G. B. Giannakis, "Distributed clustering using wireless sensor networks," *IEEE J. Sel. Top. Signal Process.*, vol. 5, no. 4, pp. 707–724, Aug. 2011.

[29] Y. Zhang, H.-C. Chao, M. Chen, L. Shu, C. hyun Park, and M.-S. Park, "Outlier detection and countermeasure for hierarchical wireless sensor networks," *IET Inf. Security*, vol. 4, no. 4, pp. 361–373, 2009.

[30] M. Xie, J. Hu, S. Han, and H.-H. Chen, "Scalable hyper-grid k-NN-based online anomaly detection in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 8, pp. 1661–1670, Aug. 2013.

[31] S. Siripanadorn, W. Hattagam, and N. Teaumroong, "Anomaly detection in wireless sensor networks using self-organizing map and wavelets," *Int. J. Commun.*, vol. 4, no. 3, pp. 74–83, 2010.

[32] S.-J. Yim and Y.-H. Choi, "An adaptive fault-tolerant event detection scheme for wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2332–2347, 2010.

[33] Y. Yao, A. Sharma, L. Golubchik, and R. Govindan, "Online anomaly detection for sensor systems: A simple and efficient approach," *Perform. Eval.*, vol. 67, no. 11, pp. 1059–1075, 2010.

[34] A. B. Sharma, L. Golubchik, and R. Govindan, "Sensor faults: Detection methods and prevalence in real-world datasets," *ACM Trans. Sen. Netw.*, vol. 6, no. 3, pp. 1–39, 2010.

[35] O. Salem, Y. Liu, and A. Mehaoua, "A lightweight anomaly detection framework for medical wireless sensor networks," in *IEEE Wireless Commun. Network. Conf.*, 2013, pp. 4358–4363.

[36] M. Weeks, *Digital Signal Processing Using MATLAB and Wavelets*. Burlington, MA, USA: Jones and Bartlett, 2006.

[37] J. Tang and Y. Cheng, "Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks," in *Proc. IEEE Int. Conf. Commun.*, 2011, pp. 1–5.

[38] Physionet. (2014). [Online]. Available: http://www.physionet.org/physiobank/database/mimicdb

[39] S. V. Aelst and P. Rousseeuw, "Minimum volume ellipsoid," *Computat. Statist.*, vol. 1, no. 1, pp. 71–82, 2009.

[40] P. J. Rousseeuw and K. V. Driessen, "A fast algorithm for the minimum covariance determinant estimator," *Technometrics*, vol. 41, no. 3, pp. 212–223, 1999.

[41] M. Huberta, P. J. Rousseeuw, and T. Verdoncka, "A deterministic algorithm for robust location and scatter," *J. Computat. Graph. Statist.*, vol. 21, no. 3, pp. 618–637, 2012.

[42] Q. Li and G. D. Clifford, "Signal quality and data fusion for false alarm reduction in the intensive care unit.," *J. Electrocardiol.*, vol. 45, no. 6, pp. 596–603, 2012.

[43] F. Schmid, M. S. Goepfert, and D. A. Reuter, "Patient monitoring alarms in the ICU and in the operating room," *Crit. Care*, vol. 17, no. 2, 2013.

[44] A. Burns, B. R. Greene, M. J. McGrath, T. J. O'Shea, B. Kuris, S. M. Ayer, F. Stroiescu, and V. Cionca, "SHIMMER™—A wireless sensor platform for noninvasive biomedical research," *IEEE Sens. J.*, vol. 10, no. 9, pp. 1527–1534, Sep. 2010.

Osman Salem received the M.Sc. and Ph.D. degrees in computer science from Paul Sabatier University, Toulouse, France, in 2002 and 2006, respectively.

He was a Researcher in the Department of Computer Science at Telecom Bretagne, France, from 2006 to 2008. Since September 2008, he has been an Associate Professor at University of Paris Descartes, Paris, France. His research interests include security and anomaly detection in medical wireless sensor networks.

Yaning Liu received the Ph.D. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2010, and from Telecom Bretagne, France, in 2011.

She was a Postdoctoral Researcher at INRIA, France, from 2011 to 2012, and joined JCP-Consult R&D, Rennes, France, in 2013. Her research interests include content centric networking, energy efficient network, peer-to-peer streaming systems, and network measurement.

Ahmed Mehaoua received the M.Sc. and Ph.D. degrees in computer science from the University of Paris, Paris, France, in 1993 and 1997, respectively.

He is currently a Full Professor of computer communication in the Faculty of Mathematics and Computer Science, University of Paris Descartes, Paris, France. He is also the Head of the Department of Multimedia Networking and Security at the LIPADE, a governmental computer science research center in Paris, France. His research interests include wireless healthcare systems and networks and applications.

Raouf Boutaba (F'12) received the M.Sc. and Ph.D. degrees in computer science from the University Pierre & Marie Curie, Paris, France, in 1990 and 1994, respectively.

He is currently a Professor of computer science at the University of Waterloo, Waterloo, ON, Canada. His research interests include resource and service management in networks and distributed systems. He is the Founding Editor-in-Chief of the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, a post which he held from 2007 to 2010, and is on the editorial boards of other journals. He is a Fellow of the Engineering Institute of Canada.

Dr. Boutaba has received several best paper awards and other recognitions such as the Premier's Research Excellence Award, the IEEE Hal Sobol Award in 2007, the Fred W. Ellersick Prize in 2008, and the Joe LociCero and the Dan Stokesbury awards in 2009, the Salah Aidarous Award in 2012, and the 2014 McNaughton Gold Medal.