Information Sciences 384 (2017) 281–297

Contents lists available at ScienceDirect

Information Sciences

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

Online personal risk detection based on behavioural and physiological patterns

Ari Yair Barrera-Animas[a], Luis A. Trejo[a,*], Miguel Angel Medina-Pérez[a], Raúl Monroy[a], J. Benito Camiña[a], Fernando Godínez[b]

[a] Tecnologico de Monterrey, Escuela de Ingeniería y Ciencias, Carretera al Lago de Guadalupe Km. 3.5, Atizapán de Zaragoza, Estado de México, C.P. 52926, Mexico
[b] Microsoft. 1 Microsoft WayRedmond WA, 98052, United States

ARTICLE INFO

Article history:
Received 31 October 2015
Revised 22 July 2016
Accepted 3 August 2016
Available online 3 August 2016

Keywords:
Pattern recognition
Physiological patterns
Behavioural patterns
Personal risk detection
Anomaly detection
One-class classification

ABSTRACT

We define personal risk detection as the timely identification of when someone is in the midst of a dangerous situation, for example, a health crisis or a car accident, events that may jeopardize a person's physical integrity. We work under the hypothesis that a risk-prone situation produces sudden and significant deviations in standard physiological and behavioural user patterns. These changes can be captured by a group of sensors, such as the accelerometer, gyroscope, and heart rate. We introduce a dataset, called PRIDE, which provides a baseline for the development and the fair comparison of personal risk detection mechanisms. PRIDE contains information on 18 test subjects; for each subject, it includes partial information about the user's behavioural and physiological patterns, as captured by Microsoft Band©. PRIDE test subject records include sensor readings of not only when a subject is carrying out ordinary daily life activities, but also when exposed to a stressful scenario, thereby simulating a dangerous or abnormal situation. We show how to use PRIDE to develop a personal risk detection mechanism; to accomplish this, we have tackled risk detection as a one-class classification problem. We have trained several classifiers based only on the daily behaviour of test subjects. Further, we tested the accuracy of the classifiers to detect anomalies that were not included in the training process of the classifiers. We used a number of one-class classifiers, namely: SVM, Parzen, and two versions of Parzen based on k-means. While there is still room for improvement, our results are encouraging: they support our hypothesis that abnormal behaviour can be automatically detected.

1. Introduction

Rapid progress in microelectronics and computer systems in recent years has led to the development of sensors and mobile devices with unprecedented characteristics such as low cost, small size, and high computational power [6,20,22,30].

* Corresponding author.
E-mail addresses: a01373306@itesm.mx (A.Y. Barrera-Animas), ltrejo@itesm.mx (L.A. Trejo), migue@itesm.mx (M.A. Medina-Pérez), raulm@itesm.mx (R. Monroy), jb.camina@itesm.mx (J.B. Camiña), fgodinez@microsoft.com (F. Godínez).

http://dx.doi.org/10.1016/j.ins.2016.08.006

As a result, there has been rapid growth and development of sensors that can be integrated in mobile phones and wearable devices.

Over the past decade, Vital Signs Monitoring (VSM) and online Human Activity Recognition (HAR) through wearable sensors have attracted considerable interest in a variety of fields, including pervasive and ubiquitous sensing, mobile computing, context-aware computing, and ambient assisted living [1,6,20,21,23,30,34,36,37,43], with special applications in medicine, security, healthcare, entertainment, military defence, and commercial fields [1,6,10,20,22,27,29,30,35–37,43]. Gartner's 2015 Hype Cycle for emerging technologies pinpoints wearables at the peak of inflated expectations [4]. Moreover, firms like Soreon Research have forecasted an annual growth rate of 65% until 2020 for the smart wearable healthcare industry [19].

In this study, we focus on a different but related application of wearable sensors, namely *personal risk detection*. We define personal risk detection as the timely identification of when someone is in the midst of a dangerous situation, for example, a health crisis or a car accident, events that may jeopardize a person's physical integrity. Recently, we deployed a personal security solution based on mobile devices called ELISA[1] (Emergency, Positioning, and Immediate Assistance). ELISA [40] aims at significantly increasing the possibility of quickly locating and assisting a person in the case of an emergency situation, such as kidnapping, car accident, or health crisis. The current number of users is around 750 and growing. When using ELISA, an alarm is triggered manually by the user in case of imminent risk, which is then displayed in an authorized C4 (Command, Control, Communications, and Computers). However, as part of the original design, we envisioned automatic alarm generation by means of a set of wearable sensors that could consider both environmental and user health conditions.

Our ultimate goal is thus to develop a mechanism that is able to detect, in a timely fashion, when an ELISA user is under imminent risk, such as a health crisis or a car accident (for example, a turnover or a high impact crash). Our hypothesis is that a risk-prone situation produces sudden and significant deviations in standard physiological and behavioural user patterns. These changes can be captured by a group of sensors, such as an accelerometer, gyroscope, and heart rate detector.

The aim of this study is twofold. First, we introduce a dataset, called **P**ersonal **RI**sk **DE**tection (PRIDE, for short), which provides a baseline for the development and the fair comparison of risk detection mechanisms. PRIDE contains information of 18 test subjects; for each subject, it includes partial information about user's behavioural and physiological patterns, as captured by Microsoft Band®. Microsoft Band is a network of wearable sensors that monitors 3D acceleration, 3D angular velocity, heart rate, distance, skin temperature, and exposure to ultraviolet rays, among others. PRIDE records include sensor readings of not only when a test subject is engaged in ordinary daily life activities, but also when that subject is in a stressful situation, which may indicate a dangerous or abnormal condition.

We have carefully designed a number of such scenarios, in order to simulate anomalous conditions, comprising possibly risk-prone situations. The scenarios include running 100 m at maximum speed, falling backwards, and more. Further, we evaluated the following detection problem: to build a mechanism that is able to detect, in a timely fashion, when a given user is in a dangerous or abnormal situation, by identifying a clear deviation from the user's ordinary profile of behaviour. Thus, we structure personal risk detection as an anomaly detection problem. The anomaly detector is a one-class classifier, which is not trained using stress scenarios; it is trained only with a user's ordinary conditions data. Stress scenarios are only used to verify if the classifier is capable of identifying them as an anomaly, and not to identify which scenario/activity is being observed. The stress scenarios are thus intended to simulate certain danger or abnormal behaviour; however, we acknowledge they are only an approximation to real-life situations. Our aim is to detect anomalies that can be the result of a car accident, health crisis, robbery, and so on. Since we do not have the means to capture data during a real crisis situation, we decided to undertake this approach.

The second aim of this paper is to show how to use PRIDE to address the above stated anomaly detection problem; to accomplish this, we have tackled risk detection as a one-class classification problem. We trained several classifiers based solely on the daily behaviour of users. Next, we tested the performance of the classifiers to detect anomalies that we did not include in the training process of the classifiers. We tested SVM [41], Parzen classifier [9], and two versions of Parzen based on k-means [13,39]. While there is still room for improvement, our results are encouraging. We have successfully validated our working hypothesis, namely that, a one-class classifier is able to detect anomalies in the sensor information of a test subject, as provided by MS Band, for personal risk detection.

It is worth noting that anomalous situations may sometimes be related to a dangerous situation, *i.e.*, to a personal risk-prone situation. However, tagging a behaviour as abnormal does not always imply risk. Furthermore, not all risk-prone situations always translate into abnormal behaviour, at least with the technology used in this study. In other words, we are able to differentiate abnormal behaviour and ordinary behaviour, thereby detecting some (but not all) possible risk-prone situations.

Paper overview. In Section 2, we review state-of-the-art approaches in HAR and VSM including some applications; additionally, we describe some popular datasets in the area. We also review the main algorithms from the machine learning and pattern recognition domains that are applied to HAR and VSM systems. In Section 3, we describe PRIDE, a new dataset publicly available for personal risk detection. Therein, we briefly describe the procedure to capture test subject data, as well as the mobile application and sensor network used during the process. In Section 4, we present our proposal for

[1] http://elisa-tec.mx