Pocket Guard – IoT-ready, Low-cost Personal Belongings Monitoring

Christian Becker Pepino
Universidade Tecnológica
Federal do Paraná
Curitiba, Paraná, Brazil

Guilherme Dias
Universidade Tecnológica
Federal do Paraná
Curitiba, Paraná, Brazil

Daniel Fernando Pigatto
CPGEI/DAELN
Universidade Tecnológica
Federal do Paraná
Curitiba, Paraná, Brazil
pigatto@utfpr.edu.br

***Abstract*—This paper presents the development of a low-cost system for tracking and monitoring personal belongings, using the concept of the Internet of Things. The system is composed of three separate parts: a prototype based on the Arduino platform, connected to Bluetooth, GNSS/GSM and accelerometer modules; an iOS mobile app with a graphical user interface that allows the prototype configuration and monitoring; and, lastly, a server to be the interface between the application and the prototype. Results prove the possibility of implementing an accurate, robust, and low-cost IoT-ready device, which can be used as a tracker for personal belongings.**

I. Introduction

Despite the evolution of electronics security and monitoring systems, microelectronics and telecommunications, there are very few practical and portable solutions for monitoring belongings. In fact, there are several security systems for real estate, cars and luxury objects, which implement typical formulas with features such as security cameras and positioning trackers, and are usually fixed and physically coupled to their objects of interest through a manual installation process. The whole process results in expensive solutions.

The main purpose of this paper is to create a module flexible enough to be easily coupled to different objects of interest, allowing micromonitorings anywhere anytime. Moreover, associate rich interfaces to help tracking the personal objects in real time. The monitoring system should become part of its user's life, being integrated to the daily routine just any other mobile devices (such as smartphones, wearable technologies and tablets). It may also be used in the future by people or institutions which need cheaper solutions to monitor critical environments, such as data centres.

II. Related Works

Autotrac Mini [1] and Apeggo [2] trackers operate based on location. They have GPS (Global Positioning System) modules, mobile applications to perform monitoring, and monthly or yearly subscription plans. In addition, they require the purchase of the tracking hardware that is coupled to the object/person monitored, which represents an extra cost.

TrackR [3] is a key ring that uses Bluetooth and connects to the user's smartphone through a phone app. By monitoring the intensity of the communication signal, the smartphone can measure the approximate distance of the device. However, if the device is out of the smartphone range, it sends a message to the TrackR server indicating the lost device ID; the server will send the lost device ID to other phones that have TrackR's app installed and are currently in the same region; then, if any of these smartphones detect the lost device, it notifies the server with its location; and, finally, the server notifies the owner with the device location. A natural disadvantage of this approach is that in some regions where there are few or no users with TrackR's app installed, the lost device will hardly be found.

There are several ways to detect potential theft (of objects) or accidents (in the case of people life monitoring) activities. Authors in [4] and [5] proposed solutions that monitor objects which are registered and equipped with RFID (Radio-Frequency IDentification), and located within the coverage area of a monitoring centre. The use of technologies such as RFID or Bluetooth to identify if an object is being moved away from the owner may be relevant for most situations, but they do not cover all cases. For instance, an unauthorised person may pick up a cell phone, have access to the owner's personal information, and do all of this while keeping the device within the coverage area of a monitoring centre, thus generating no alert at all. A second example may occur when an elderly person who uses a monitoring device suffers a fall and does not receive care due to the non-identification of the occurrence by a system based on short-range communication.

Therefore, the use of short-range wireless technologies associated with an accelerometer represents an adequate way of identifying the unauthorised use of devices and occurrences with people, as well as identifying possible thefts. An implementation with low cost sensors and own server also helps towards the reduction the costs, allowing greater accessibility to the product. Thus, the main objective of this paper is to create a new low-cost tool for the security of personal objects and/or systems. It encompasses a motion sensor (accelerometer), GSM (Global Systems for Mobile communications) communication module, Bluetooth communication module and GNSS module. The device connects to a web server that interfaces the communication with a smartphone, where the user can configure several devices and get notifications of suspicious events in the monitoring network.

III. Pocket Guard

A. System description

Pocket Guard is a tracking system composed of a handheld device connected to the Internet, a web server and a smartphone app. The prototype is an Arduino micro-controller that can be positioned by the user in any of its properties, such as a purse or backpack, a car, in the drawers of a furniture, etc. Once activated, the device turns on its accelerometer and, if it detects an atypical pattern of movement, potentially corresponding to a theft, it notifies the user immediately. The notification is displayed on the user's smartphone screen, accompanied by a sound indication. The user can then open the app and track the belonging location in real time.

In order to use the system, the user needs the Pocket Guard app and own a portable Pocket Guard tracking device with an active GSM chip inserted. There are no buttons or screens that display information directly on the tracker, so all device monitoring and configuration is done through the Pocket Guard application. A login screen guides the user through processes of registration/login, as shown in Figure 1.

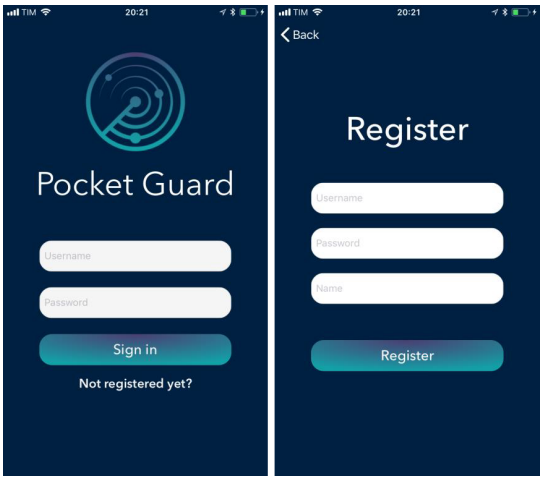

Fig. 1: Pocket Guard sign-in and sign-up screens.

After registering, the user can login and pair the first device. To perform pairing, it is needed to simply turn on Pocket Guard device, open the pairing screen on mobile app, and click the pair button. After that, the user should only position the device at the location of interest. After that, the system is active and ready to monitor the accelerometer movement signals, its geographical position via GNSS and measure the distance from the user's smartphone via Bluetooth, sending reports to the server periodically[1]. Figure 2 shows the app's main screen with a registered device.

The system constantly monitors the device. If it determines that the device is away from the user, a simple alert is sent to the smartphone app. From this moment on, if any drastic movement is detected, the system starts the alarm trigger mode. That generates a notification which is immediately sent

[1]The frequency can be configured by the user.

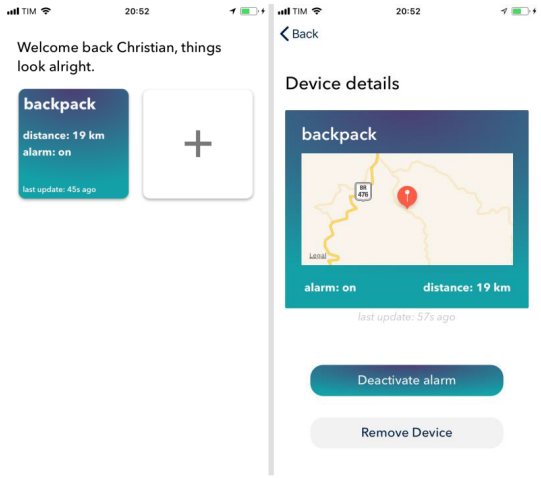

Fig. 2: Main screen listing tracked devices details.

to the user, with constant updates containing geographic positions. Figure 3 shows screen captures with the aforementioned notifications.

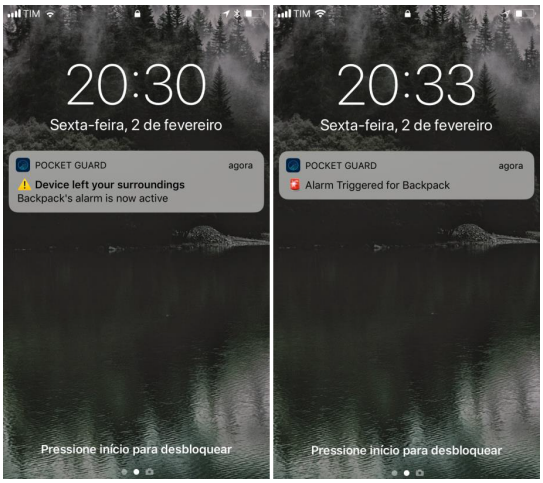

Fig. 3: Proximity and alarm trigger notifications.

The Pocket Guard app and the tracking device communicate via Bluetooth and determine the distance between them, always assuming that the tracker owner is carrying its own smartphone. Both the app and the device periodically communicate with the server by sending HTTP (Hypertext Transfer Protocol) requests with status updates, as shown in Figure 4.

The main functionalities of the Pocket Guard system are the detection of movement of the tracking device using the accelerometer; communication of the device with the server through a GPRS network; tracking the device through the GNSS system; an app for user registration and administration; and proximity detection between the smartphone and the pairing device via Bluetooth.

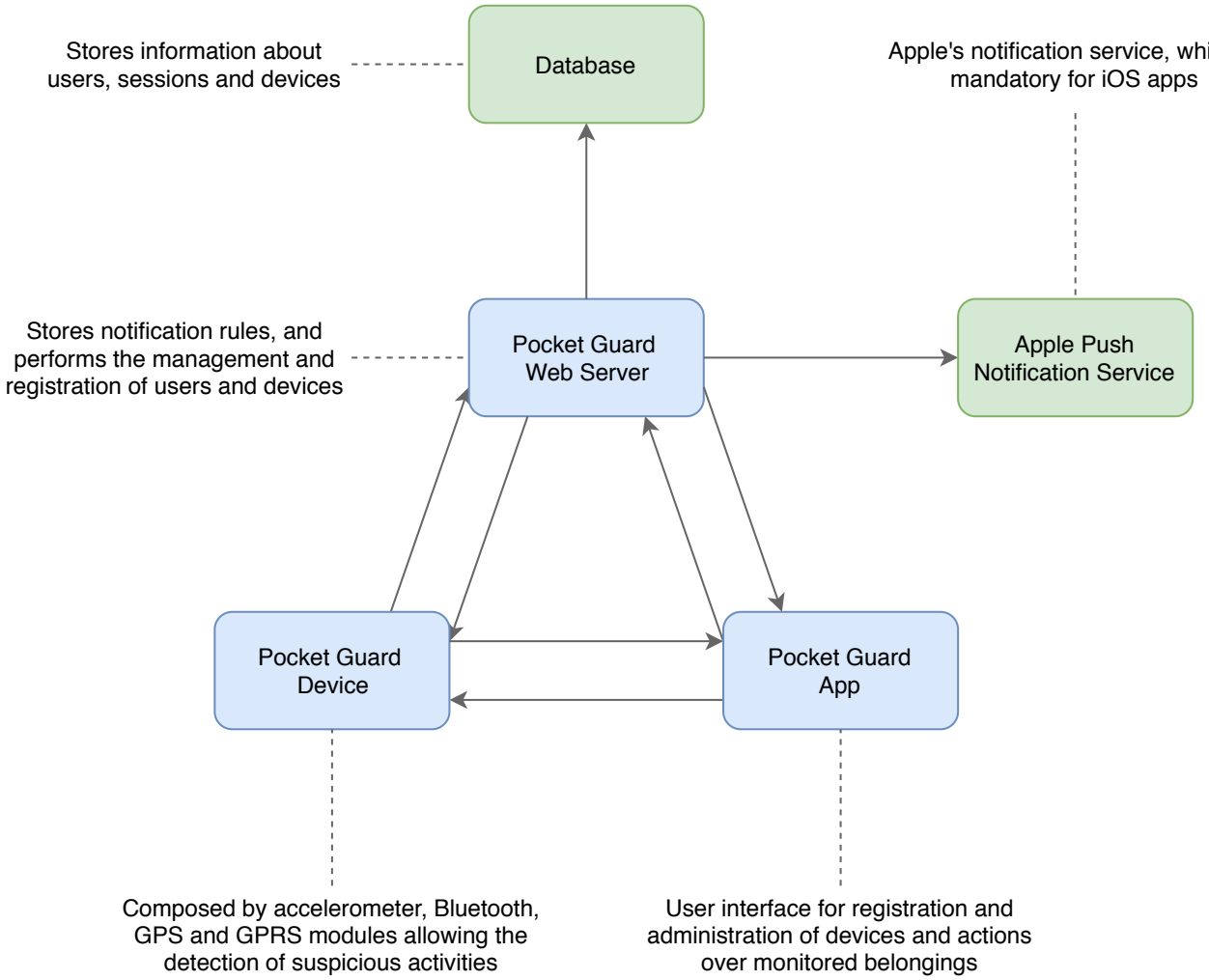

Fig. 4: General diagram of the Pocket Guard system.

B. Hardware prototype

The motherboard used was the Arduino UNO Rev3, due to its simplicity and lower cost among Arduino series. A MPU 6050 module was used for accelerometer measurements, a HM-10 BLE module for Bluetooth and a SIM 808 module was used for GPS and GNSS. The system was implemented following the state machine concept. Four states have been defined: Active, Alarm, Proximity and Pairing. A state machine diagram is presented in Figure 5, which contains 4 states:

- The *Active* state is started when the user turns on the device. If the device has already been configured, the system continuously checks the accelerometer data. Then, if the accelerometer values indicate a suspicious movement, the system changes the state to *Alarm*. Based on Bluetooth information, the device can determine if the user is nearby and change its status to *Proximity*.
- In the *Alarm* state, the device checks the accelerometer and sends a notification on the smartphone app indicating the suspicious activity. The user then receives GNSS data indicating the current position of the device.
- In the *Proximity* state, enabled by detecting that the device is close to the user, the device stops scanning the accelerometer and deactivates the SIM 808 module, which manages GPRS and GNSS communication. As soon as the device moves away from the user, the device returns to the *Active* state, and the user is notified about this.
- Finally, the last state is the *Pairing*, in which the device was not yet paired with any user. In this state, the device constantly scans the readings of the Bluetooth module to find any nearby handsets to connect. When paired with a smartphone, the device switches to the *Active* state.

IV. Web server development

For the execution of this project, it was necessary to create a web server to mediate communication between the tracking device and the application, also for authentication and storage of user data, device management and notification triggering. Node.js was used for the implementation of the web server. Its architecture is event-driven, which enables asynchronous input and output management, thus increasing server capacity and

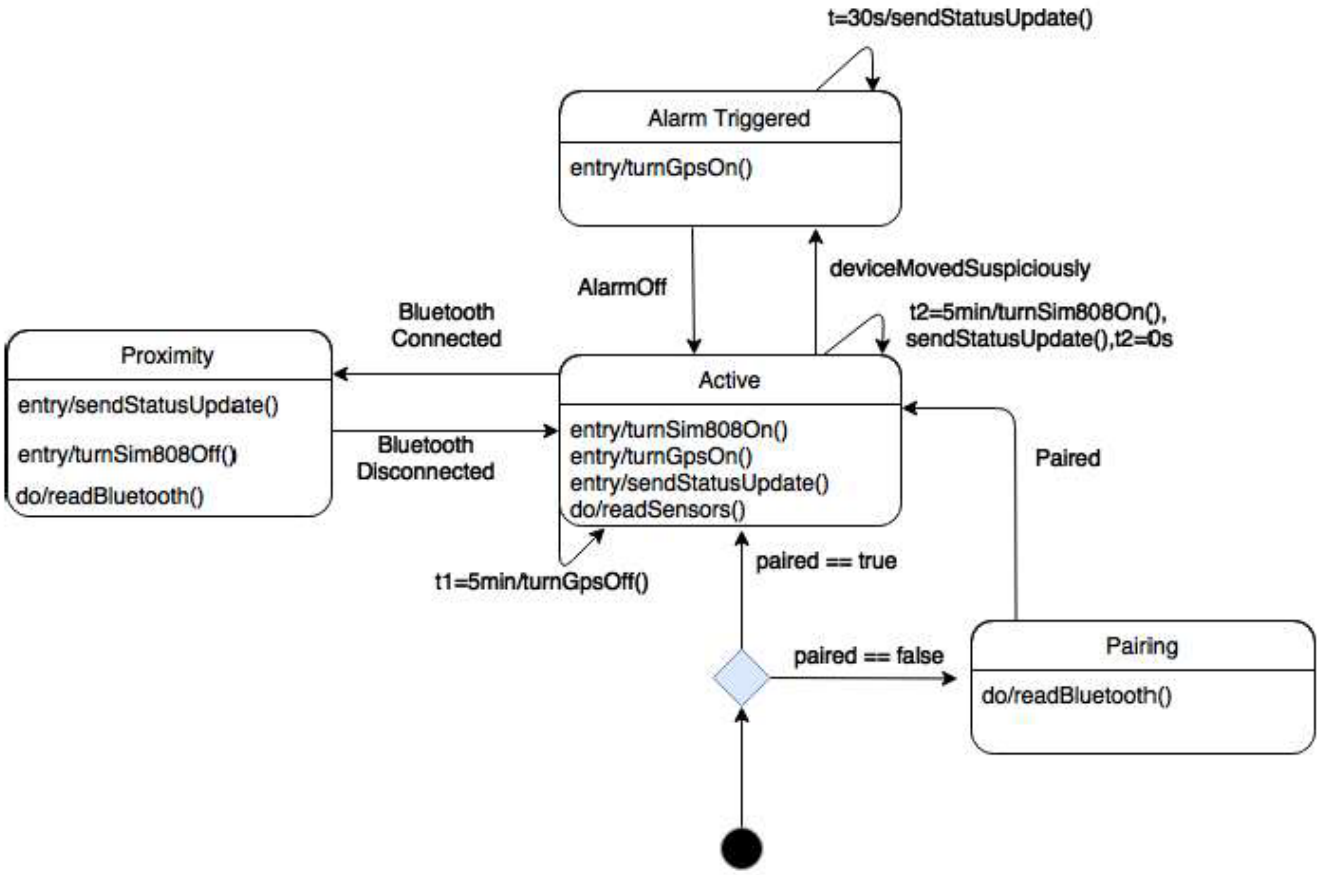

Fig. 5: State machine diagram used for the prototype implementation.

scalability. A thread dispatches individual events by pulling them out of a global queue and executing one at a time.

Messages among the device and/or the user's smartphone with the server follow Javascript Object Notation (JSON) format, a clean, human-readable data encapsulation format. It supports vectors, key and value dictionaries, and pure data types such as strings and numbers. The database chosen for storing users and devices data is MongoDB.

The hosting service used was Heroku, a platform that supports several programming languages, including Javascript. It has been chosen among other options due to the quality of its service and the facility of uploading an application, as well as the free tools provided, such as a custom command line interface.

To send notifications to the user, a bridge was created between the Pocket Guard server and the Apple Push Notification Service, which is the centrepiece of the Apple device notification system.

V. Results evaluation

As previously shown, Pocket Guard can be used to monitor personal belongings or objects to which the prototype can be affixed. The developed prototype can be seen in Figure 6.

Some situations where Pocket Guard may be applied are on tracking backpacks and cars. Figures 7 and 8 show the prototype in these situations.

In both situations, it was possible to identify suspicious activities and report the device owner. Also, as soon as the device is moved away from the owner's smartphone, the tracking system started to inform in real time the belonging positioning. These experiments have proved that Pocket Guard can be used to track personal objects with a low cost solution.

VI. Conclusions

The objective of this work was the development of an IoT-ready prototype for a monitoring system, which was satisfactorily achieved. A complete portable tracking solution based on an app and a tracking device was created, connected by a centralised web service.

The novelty is the portability of the system, the mobile app and the low power consumption. The architecture centralises the app logic in the service, as well as the communication between smartphone and device, through a RESTful API. However, in some opportune moments, there is also direct communication between the app and the device.

Using low power states, it was possible to reduce the energy consumption of the device prototype, allowing a few extra time for battery autonomy. To achieve this result, we have

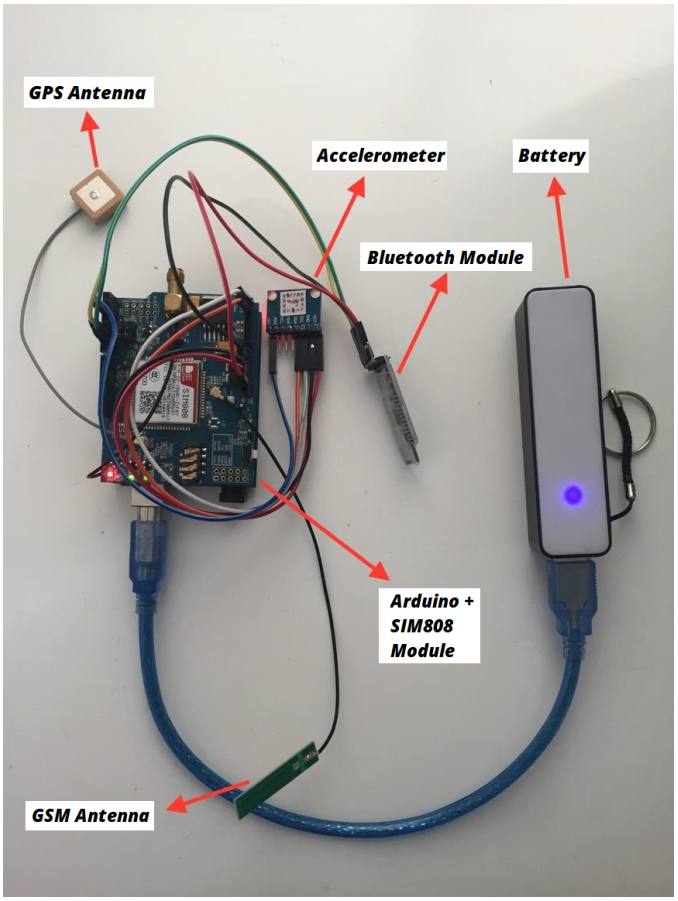

Fig. 6: General prototype of the Pocket Guard device.

Fig. 7: Pocket Guard device coupled to a backpack.

implemented the detection of user's presence near the tracked device tracker, deactivating some features and reducing the energy consumption to the minimum possible.

As future work we intend to improve the communication between the device, the smartphone and the server, in order to reduce delays and encrypt messages, providing better security

Fig. 8: Pocket Guard device inside a car.

and reliability to the system. It is also important to implement the firmware of the device using a Real-Time Operating System (RTOS), allowing different degrees of priority. Finally, an Android app would allow more users to use Pocket Guard.

REFERENCES

[1] Autotrac, "Autotrac Mini," 2018. [Online]. Available: http://www.autotrac.com.br/produtos/mini/

[2] Appego, "Appego GPS," 2018. [Online]. Available: http://www.meappego.com.br/

[3] TrackR, "TrackR," 2018. [Online]. Available: https://secure.thetrackr.com/

[4] S. Chan, A. Connell, E. Madrid, D. Park, and R. Kamoua, "RFID for personal asset tracking," in *2009 IEEE Long Island Systems, Applications and Technology Conference*. IEEE, may 2009, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/5031570/

[5] W. Zheng, X. Wang, and R. Kamoua, "Personal asset tracking," in *2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, may 2013, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/6578230/