# A WIRELESS CONTROL SYSTEM BASED ON SMART BLUETOOTH AND IBEACON TECHNOLOGY FOR AUDITING THE PATROLS

Murat Karakaya, Department of Computer Engineering, Atılım University, Incek, Ankara, Turkey
Email: murat.karakaya@atilim.edu.tr

Gökhan Şengül, Department of Computer Engineering, Atılım University, Incek, Ankara, Turkey
Email: gokhan.sengul@atilim.edu.tr

Atila Bostan, Department of Computer Engineering, Atılım University, Incek, Ankara, Turkey
Email: atila.bostan@atilim.edu.tr

**Abstract:** Patrol systems are used as a method of ensuring security and protection of large areas and facilities such as university campuses, military zones, etc. In general, security personnel assigned to the patrol system visit the pre-determined checkpoints at regular intervals and are obliged to make the safety control of these locations. Security personnel (guards) are also audited to check if they covered all the essential control points on time or not. In recent years, considering energy efficiency, new Bluetooth devices and protocols are designed and produced. One of the most popular low-energy Bluetooth protocols is Smart Bluetooth (version 4.0). In this work, we integrated mobile devices (smart phone or tablet) with IBeacons. IBeacons are devices emitting beacons using Smart Bluetooth signals. Since Smart Bluetooth consumes low energy, these devices are small in size, have long life durations and very cheap. In this work, we propose and implement a new system to record the patrol officers' movements in the subject areas. At the proposed system, IBeacons are first deployed in the monitoring areas. The location and the identification of the deployed IBeacon are stored in a central database. We developed a mobile application for Android devices which can scan the environment for IBeacon signals. The mobile application collects the sensed IBeacon IDs, stamps it with a time tag and uploads it along with the mobile device ID to the central database. Using these records, we can monitor the movements of the security guards. We have also developed a web application to generate an executive summary report from these records.

***Keywords*** **–** Security, Patrol, wireless communication, mobile computing, control

## 1. INTRODUCTION

For guarding and monitoring regions and buildings, security personnel patrol the responsibility areas periodically. They can be on foot or mobilized. One administration consideration is if the staff obey the patrolling rules or not. Therefore, there are several methods put into action to monitor the patrolling activities. These methods aim to verify the actions of the security guards regarding location and time. In general, some control points (CPs) are determined in the monitored area. Security guards are supposed to visit these CPs during patrolling. The tour executed by a security guard must contain these CPs. In some cases, the order of the visited CPs might be necessary.

One of the oldest but popular methods requires deploying a notebook at each CP so that when a security guard visits that CP he or she can sign the notebook with the date and time information. These notebooks are checked periodically by a supervisor. This method is simple enough to implement with ease. Unfortunately, it does not provide sufficient measures to detect any fraud which might be done by security guards. Moreover, the manual checking of notebooks could cause waste of supervisor's time and effort.

Contrary to the manual system, in the last decade, we have witnessed many new implementations of electronic solutions such as [1-4]. In these electronic systems, new technologies have been adopted to the monitoring patrolling activities. For example, in [1], a unique device is designed to collect GPS signals to locate the security guard as seen in Figure 1. The security guard carries this handheld device, and when he or she arrives at a CP, he can scan the CP with this reader. The device records the time and date as well. Then, the collected data should be transferred to management software as seen in Figure 1.

**Figure 1.** *Embedding a GPS receiver into a reader and transferring collecting data to management software [1].*

In [2], each CP is marked with a QR code as seen in Figure 2. A mobile application is installed on smartphones to scan these QR labels when a

security guard visits a CP. Via the application, the collected data is uploaded to management software.


**Figure 2.** *Using QR codes and mobile application [2].*

In [3], a special device is designed to scan RFID and NFC signals as seen in Figure 3. Therefore, each CP is furnished with a RFID or NFC label. When a security guard carrying the device approaches to a CP, the device can capture the signal of RFID or NFC tag and transfer it to management software.


**Figure 3.** A special device to scan RFID and NFC signals *[3]*.

As the last example, in [4], the designed unique key is used to identify the CP as seen in Figure 4. This device can scan RFID signals, or it can touch a special button to recognize the CP identity. After collecting information, the device is connected to a unique device to transfer the data to a computer as seen in Figure 4.

**Figure 4.** A special device to scan signals from RFID and key *[4]*.

The solutions presented above have their advantages and disadvantages. For example, when specially designed and manufactured devices are used as in [1,3,4], the cost of a solution gets higher, and the user depends on a specialized manufacturer for long-term use of the system. However, as in [2] if the system parts are generic devices such as smartphones and some radio emitters, then system can be realized by purchasing these elements from an open market which reduces the cost-effectively. Besides the cost and sustainability, another important design parameter of such a system is the security of the solution. For example, in [2], one can deceive the system using a replicated QR code instead of QR code deployed at the CP.

As discussed above, new technologies enable us to design new systems for monitoring patrolling activities. In this paper, we propose a novel system using Smart Bluetooth (namely, Low Energy Bluetooth) technology and present the initial findings of its implementation. The details of the proposed system are given in the following sections.

## 2. USING SMART BLUETOOTH TECHNOLOGY

In this section, we first provide the details about the underlying Bluetooth technology and Bluetooth enabled tags. Then, we explain the advanced mobile application and management software. In the end, we provide a discussion about the initial experiences from the pilot deployment.

### 2.1. Smart Bluetooth

Bluetooth 4.0 is the latest version of the wireless technology found in many electronic devices and peripherals today, including smartphones and watches, and it is designed by The Bluetooth Special Interest Group [5]. In general, compared to the previous version of Bluetooth technology, Bluetooth 4.0 improves considerably power consumption by implementing a more energy-efficient signaling method which keeps paired devices connected without the need for a continuous information stream.

Bluetooth 4.0 introduces two types of devices: Bluetooth Smart and Bluetooth Smart Ready. Bluetooth Smart is specially designed for sensor-type devices like heart-rate monitors or pedometers that run on small batteries which collect specific pieces of information. These Bluetooth Smart devices include a single Bluetooth 4.0 radio that will connect only to Bluetooth Smart Ready devices. Thus, we can state that Bluetooth Smart Ready is for server-type devices which have better energy resources.

As a result of two different implementations and hardware, sensor-type devices consumes less power when communicate and get paired to server-type devices. This innovation leads many small sensor devices to live longer with little battery capacity. Examples of these devices are smartphones and tablets. In our implementation, we choose smartphones which support Bluetooth Smart Ready and IBeacons embedded with Bluetooth Smart.

| Property | Value |
|---|---|
| Range | Up to 30 meters |
| Battery life | 18 months (max. |
| Portability | High |

### 2.2. IBeacon

IBeacon is a wireless communication protocol introduced by Apple on top of Bluetooth Smart technology [6]. These beacons emit signals periodically such that mobile applications can be aware of their whereabouts using the information broadcasted by beacons. Thus, IBeacon devices use Bluetooth Smart whereas the mobile device such as smartphones implements Bluetooth Smart Ready.
In most of the implementations, IBeacons are deployed static locations and their broadcasted identification numbers (ID) are associated with the deployment location in a database. The application running on a mobile platform such as a smartphone can receive the beacon signal and decode it to find the ID of the IBeacon to estimate its location by comparing the stored location of this IBeacon at the database. In this work, we implemented a similar approach to monitoring the security guards activities related to patrols.

## 3. A WIRELESS CONTROL SYSTEM BASED ON SMART BLUETOOTH AND IBEACON TECHNOLOGY FOR AUDITING THE PATROLS

There are several brands which produce IBeacon devices such as [7] and [8]. We opted for the ones generated by EasiBeacon company [8]. The property of the selected IBeacon is given in Table 1. As a mobile device, we use a well-known smartphone.

The system architecture is given in Figure 5. Each security guard carries a smartphone on which a unique mobile application is installed. This application scans the environment using Smart Bluetooth Ready protocol for beacons emitted by any IBeacon device. Whenever a beacon is received, the mobile application decodes the signal to determine the ID of the IBeacon and its estimated distance from the smartphone. Then, the mobile application prepares a log entry in which the identification numbers of cell phone and IBeacon, time, and the distance from the IBeacon are recorded. This log is uploaded to a central database. The management software provides the required reports.

**Table 1.** The properties of the selected IBeacon [8].

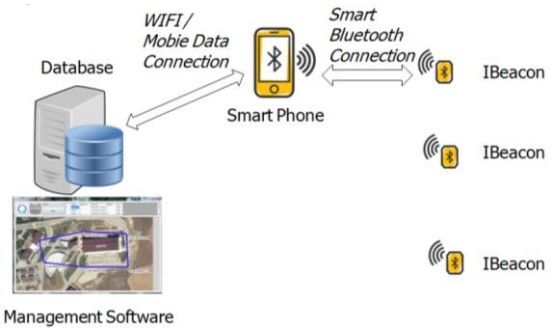


**Figure 5.** The system architecture of the proposed system.

We have developed the mobile application using Android Studio [9]. After installation, the mobile app works in the background. Thus, the security guard does not have to set up or modify anything to run the application. IBeacons are deployed at each checkpoint (CP). After deploying, IDs of IBeacons at each CP are stored in the database. Since battery life is longer compared to a smartphone, we assume that after deployment for a long time we won't have to change them. Thus, the maintenance of them would be easy.

The database is realized by using MySQL RDMS [10]. Mainly, we have three relations at the schema. The first table holds user information along with the smartphone IDs. In the second relationship, we keep the logs arrive from the smartphones. The last schema is for storing the locations of Ibeacons.
The management software is designed with Eclipse IDE [11]. As seen in Figure 6, a supervisor efficiently can produce various reports as text or graphic. The supervisor can prepare a report according to activities of a selected security guard, a selected set of CP, or a specified duration.

Moreover, the software shows real-time events as well.


**Figure 6.** Management Software of the Proposed System.

## 4. DISCUSSION AND CONCLUSIONS

In this work, we introduce a monitoring system for security guards based on Bluetooth and IBeacon technologies. We implemented the systems and experimented with it. The first observations are as follows:

- The new version of Bluetooth protocol provides reliable service regarding pairing and connection management.
- IBeacons are also reliable regarding pairing. However, the estimated distance correctness is arguable. In the outdoors, the estimations are more close to reality whereas, indoors the estimate accuracy can considerably diminish according to the surrounding environment.
- Broadcast period of IBeacons can be set. We set beacon period 1 second. In this setting their batteries last about 1 year. This duration is acceptable considering their low price.
- Management software proves its effectiveness and usefulness when used by several security guards. Especially, the presentation of real time data on a map interests all the testing personnel.
- One consideration from the security guards is the concern about the mobile application that they have to install their smartphones. They are reluctant to install it because they hesitate that this software can track them outside of the campus as well even though the system is explained well.

As a result of these observations, we aim to develop this system as a ready-to-use package for users by improving management software and security of the system.

## ACKNOWLEDGMENTS

This project is supported by Atilim University as an Undergraduate Research Project (ATÜ-LAP-C-1415-12). The student members of the project group are Fatih Demir, Mohamad Ballan, Oğuz Kaan Demirhan, Gözde Tarcan, and İnci Evrim Çamalan. We would like to extend our gratitude to all the project group student members for realizing this project.

## REFERENCES

[1] Guard Tour Systems (2016) [Online]. Available: http://guardtour.co.uk/

[2] QR-Patrol (2016) [Online]. Available: https://www.qrpatrol.com/system

[3] GuardTek (2016) [Online]. Available: http://www.trackforce.com/

[4] Palm Touch Starter Kit, Guard Patrol Products (2016) [Online]. Available: http://guardpatrolproducts.co.uk/

[5] Bluetooth Special Interest Group, (2016) [Online]. Available: https://www.bluetooth.com/

[6] iBeacon for Developers, Apple com, (2016) [Online]. Available: https://developer.apple.com/ibeacon/

[7] Estimote Beacons, (2016) [Online]. Available: http://developer.estimote.com/ibeacon/

[8] easiBeacon, (2016) [Online]. Available: http://www.easibeacon.com/doc/

[9] Android Studio, Google Inc., (2016) [Online]. Available: https://developer.android.com/studio/

[10] MySql, Oracle Inc., (2016) [Online]. Available: https://www.mysql.com/

[11] Eclipse IDE, (2016) [Online]. Available: https://eclipse.org/