Using Mobile Devices to Manage Traffic Infractions

Stefânia Marques
Federal University of Campina Grande, Brazil

Sabrina Souto
Federal University of Campina Grande, Brazil

Miguel Queiroga
Federal University of Campina Grande, Brazil

Hyggo Almeida
Federal University of Campina Grande, Brazil

Angelo Perkusich
Federal University of Campina Grande, Brazil

INTRODUCTION

Mobile computing is one of the recent technologies with the most impact on people's lives. Several research and industrial applications are benefiting from mobile computing, supporting various human daily activities. Transit law enforcement officials can benefit from the availability of powerful mobile devices, such as smart phones and PDAs, to help them to execute their daily tasks. In such a scenario, an official can verify a driver's data record and issue tickets online.

In this article we describe the SM-FIT system that makes it possible for transit law enforcement officials to perform online queries about potential infractions of a driver of a vehicle by using a mobile device. Queries are performed based on a unique identifier: the driver's license number.

The system is implemented based on a client-server paradigm, where mobile devices are clients and servers are base stations. Clients must have a local database to store each result of a query, when needed. Each registry stored has the following attributes: a unique identifier, the number of the vehicle's plate, the date and time that the officer registered the infraction, and the status of the infraction. Besides, photographs can be stored, digitally signed, and transmitted to a database for future prosecution.

The remainder of this article is organized as follows. We first outline some background concepts related to the system's development. We then present the proposed system architecture and functioning, and discuss some trends related to future research in this area. We close with some final remarks.

BACKGROUND

This section describes briefly some concepts related to J2ME and, more specifically, MIDlets. Such technologies have been used for developing the proposed system.

J2ME

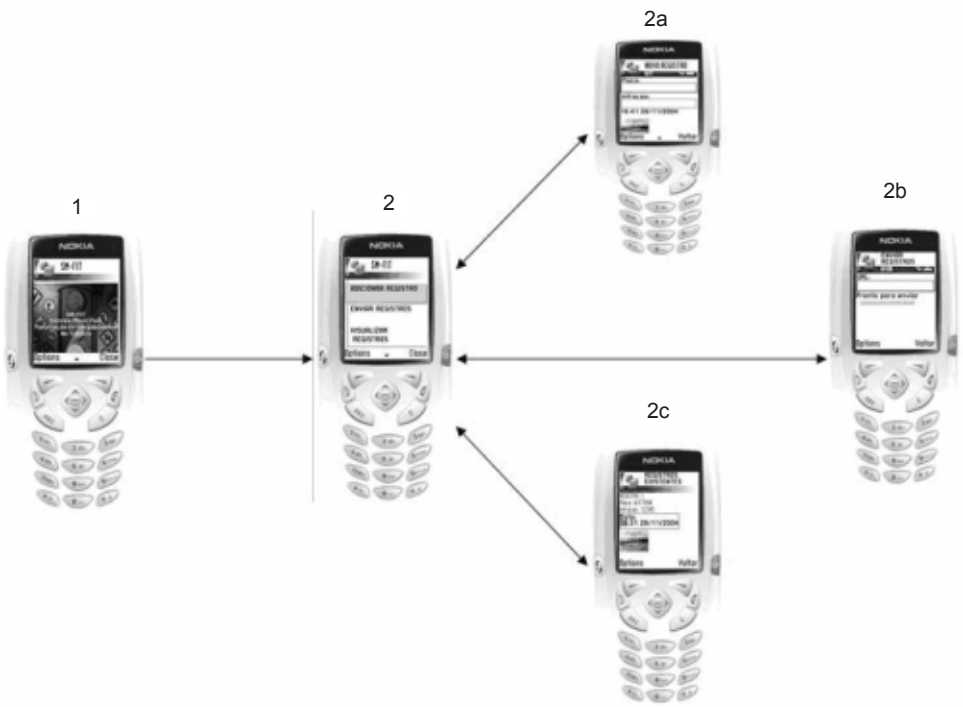
J2ME is a development platform based on Java Technology for developing mobile and embedded applications. It focuses on two types of devices:

- **High-End Consumer Devices:**
  - CDC (connected device configuration);
  - interactive TVs, videophones, wireless devices;
  - a large variety of user interfaces;
  - typical memory of 2 to 4 Mb; and
  - persistent connection, generally TCP/IP.
- **Low-End Consumer Devices:**
  - CLDC (connected limited device configuration);
  - cell phones, bidirectional pagers, PDAs, and so forth;
  - limited processors (8 to 32 MHz);
  - limited memory;
  - lazy connection, intermittent (9600bps) and generally not based on TCP/IP; and
  - powered by batteries.

The J2ME platform includes flexible user interfaces, a robust security model, a broad range of built-in network

Copyright © 2007, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

Figure 1.



protocols, and extensive support for networked and off-line applications. Besides this, applications based on J2ME specifications are written once for a wide range of devices.

MIDlets

Java applications running on MIDP devices are known as MIDlets, which consist of at least one Java class and have to be derived from the abstract class javax.microedition.midlet.*MIDlet*. These MIDlets use an execution environment within the Java Virtual Machine to control the application's lifecycle through a set of methods implemented by this MIDlet.

MIDlets can also use methods to obtain services from the environment. A group of related MIDlets can be put together in a MIDlet suite, which is packaged and installed in (or removed from) a device as a unique entity. MIDlets in a suite share all static and dynamic resources in their environment:

- Execution data can be shared by MIDlets, and the usual Java conventions of synchronization can be used to control data access.
- Persistent data can also be accessed by all MIDlets in a suite.

All files in a MIDlet suite must be within a JAR package. These packages contain the classes of the MIDlet and other resources, like images, and a manifest file. This manifest file contains a list of attributes and definitions to be used by application managers to install the JAR files in the device.

Security in MIDlets

The JAVA security model in its standard edition (J2SE) is too expensive in terms of costs for memory allocation, and it requires configuration knowledge that is not present in users of mobile devices. Thus, neither CLDC nor MIDP include these functionalities.

Cryptography of public key and certifiers are not available as default, so it is necessary to pay attention when installing MIDlets and, preferentially, only accept software from trustable fonts. MIDP 2.0 included the https protocol that helps to diminish these problems.

SYSTEM DESCRIPTION

The SM-FIT is a system that makes it possible for transit law enforcement officials to register transit irregularities in a local database. Each record of this database consists of the number of the vehicle's plate, a code of the infraction, date and time that the infraction occurred, and the photography of the vehicle involved in the corresponding infraction.

1 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/using-mobile-devices-manage-traffic/17205

Related Content

Security Model of Internet of Things Based on Binary Wavelet and Sparse Neural Network
Zhihui Wang, Jingjing Yang, Benzhen Guoand Xiaochun Cheng (2019). *International Journal of Mobile Computing and Multimedia Communications (pp. 1-17).*
www.irma-international.org/article/security-model-of-internet-of-things-based-on-binary-wavelet-and-sparse-neural-network/220419

Cyberinfrastructure, Cloud Computing, Science Gateways, Visualization, and Cyberinfrastructure Ease of Use
Craig A. Stewart, Richard Knepper, Matthew R. Link, Marlon Pierce, Eric Wernertand Nancy Wilkins-Diehr (2019). *Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics (pp. 157-170).*
www.irma-international.org/chapter/cyberinfrastructure-cloud-computing-science-gateways-visualization-and-cyberinfrastructure-ease-of-use/214612

Distributed Approach for QoS Guarantee to Wireless Multimedia
K. Chetan, P. Venkataramand R. Sircar (2007). *Encyclopedia of Mobile Computing and Commerce (pp. 195-201).*
www.irma-international.org/chapter/distributed-approach-qos-guarantee-wireless/17076

Machine Learning Based Prediction and Prevention of Malicious Inventory Occupied Orders
Qinghong Yang, Xiangquan Hu, Zhichao Chengand Kang Miao (2014). *International Journal of Mobile Computing and Multimedia Communications (pp. 56-72).*
www.irma-international.org/article/machine-learning-based-prediction-and-prevention-of-malicious-inventory-occupied-orders/144445

A Trustworthy Usage Control Enforcement Framework
Ricardo Neisse, Alexander Pretschnerand Valentina Di Giacomo (2013). *International Journal of Mobile Computing and Multimedia Communications (pp. 34-49).*
www.irma-international.org/article/trustworthy-usage-control-enforcement-framework/80426